2017 IEEE 35th International Conference on Computer Design

Implications of Distributed On-Chip Power Delivery on EM Side-Channel Attacks

Ahmed Waheed Khan
Electrical Engineering
University of South Florida
Tampa, USA
ahmedwaheedk@mail.usf.edu

Tanya Wanchoo
Intel Corporation
Folsom, USA
tanya.wanchoo@intel.com

Gokhan Mumcu
Electrical Engineering
University of South Florida
Tampa, USA
mumcu@usf.edu

Selçuk Köse
Electrical Engineering
University of South Florida
Tampa, USA
kose@usf.edu

***Abstract*—EM side-channel leakage is typically the derivative of the power consumption profile of a circuit. Since the fluctuations of the supply voltage strongly depend on the topology and characteristics of the power distribution network (PDN), the design of the PDN has a direct impact on the EM side-channel leakage signature. In this paper, the security implications of distributed on-chip voltage regulators against EM side-channel attacks are investigated. Extensive HFSS simulations have demonstrated that the maximum EM radiation can be reduced by 33 dB and 11 dB, respectively, at the front and back sides of an integrated circuit with distributed on-chip voltage regulation since the power is delivered locally through partially shorter and thinner metal lines as compared to the designs with off-chip voltage regulators.**

***Keywords*-EM side-channel attacks; distributed voltage regulation; on-chip power delivery.**

I. Introduction

Side channel attacks (SCA) are a serious threat to the security of cryptographic devices. A significant amount of work has been performed on SCAs over the past two decades. One of the primary types of SCAs is the power analysis attack. While simple power analysis (SPA) obtains the data directly from the power consumption, differential power analysis (DPA) attacks require certain statistical operations on a large number of power traces to get the relevant information [1]–[3]. Apart from the power consumption, other leakage information such as electromagnetic emissions, memory access times, and temperature can also be used to attack a device [5]–[7]. SCA tries to determine the correlation between any kind of side channel leakage profile and the internal operations of the device.

In circumstances where a power side channel is not possible or a non-contact type of attack needs to be implemented, electromagnetic (EM) attacks offer an advantage over conventional power analysis attacks. Additionally, as described by Agrawal *et al.* [8], EM attacks can also be used to nullify some of the countermeasures that are effective against power analysis attacks. Analogous to SPA and DPA, EM side channel attacks can be used to perform simple electromagnetic (SEMA) or differential electromagnetic (DEMA) attacks. While near-field probes could be used to detect emissions in the near field, larger antennas can be used to capture information bearing signals from a distance, making the EM attacks non-invasive.

The amplitude of the EM radiation is proportional to the dimensions of the current carrying wires in the circuit under attack. Longer interconnect wires emit greater EM signals, resulting in a higher amount of leakage. As the conducting wires become shorter and narrower, the EM radiation reduces, making it more difficult for the attacker to obtain sufficient level of useful information to perform a successful EM attack. Therefore, utilizing shorter interconnect wires can help in minimizing the unintentional leakage of critical side channel information. With these factors in mind, distributed on-chip voltage regulators may potentially provide certain inherent security benefits against EM attacks. Additionally, tailoring the placement of capacitors in the power delivery network can further mitigate the EM side-channel leakage.

Recently, several techniques have been proposed to implement voltage regulators fully on chip to obtain faster voltage scaling and multiple power islands [15]–[19]. This paper aims to analyze the implications of an on-chip power delivery on EM emissions. On-chip voltage regulation enables the utilization of shorter and thinner interconnect wires to deliver power as compared to off-chip regulators [9]. Additionally, various design options such as placing voltage regulators close to the cryptographic module and locally delivering power to the crypto circuit through the bottom metal layers are examined in this paper with the aim of making detection of EM radiation by any probe difficult [20].

The remaining part of the paper is organized as follows. EM attacks are explained in Section 2 and the threat model is provided in Section 3. A brief background for on-chip power delivery is given in Section 4. The evaluation of the security implications is provided in Section 5. A brief discussion on the practical considerations and noise impact of utilizing local power grid lines are also offered in Section 5. Finally, the paper is concluded in Section 6.

1063-6404/17 $31.00 © 2017 IEEE
DOI 10.1109/ICCD.2017.57

II. Electromagnetic attacks

Electromagnetic emanations carry significant information about the information being executed on the circuit. Considering a wire of length L, carrying constant current I, the magnetic field B is calculated at a point along the middle of the wire at a distance R, using Biot Savart's Law [21].

$$B = \frac{\mu_0 I}{4\pi R}\left(\frac{L}{\sqrt{L^2/4 + R^2}}\right) \tag{1}$$

where μ_0 is the magnetic constant.

The electric field generated can be approximated to be a cylindrical Gaussian surface.The Gaussian cylindrical surface is assumed to be coaxial with the wire of radius R and length L.

$$\phi E = E\int dA \approx E(R)(2\pi RL) \tag{2}$$

where $E\int dA = Q_{in}/E_0$ and Q_{in} is the new charge inside the Gaussian surface (λL).

The power consumption of cryptographic circuits is a function of the data that is being processed during encryption or decryption, contributing to the change of EM emanations from cryptographic engines. Modern integrated systems potentially generate a greater amount of side-channel leakage due to the high operating frequency, more number of pins serving as external antennas, and higher voltage levels [22]. There are two broad classifications of EM emanations, direct emanations resulting from intentional current flows and indirect emissions that are generated due to power consumption of different blocks. For example, the variations in power consumption patterns due to switching operations in a crypto circuit lead to these unintentional radiations, which may aid an attacker in obtaining useful information about the encryption algorithm being executed within the target circuit. The radiations are also produced from the inadvertent electromagnetic coupling between different components on a chip [8], [23]. Due to the rapid changes in the current, the EM field surrounding the chip varies and can be monitored by sensitive probes [23]. However, these probes have to be placed in close proximity to the source as the signal is mixed with interference from the neighboring components. In the subsequent sections, we demonstrate that incorporating on-chip voltage regulators significantly reduces these EM emanations. As the required power is delivered from the voltage regulators to the load circuits through local, thinner metal lines, the detection of the corresponding EM emanations becomes difficult.

A. Near-field and far-field approximations

The electromagnetic behavior of EM emitting sources can be studied by defining near field and far field approximations.

Near-field: With the wave number $k = 2\pi/\lambda$, the near field region is characterized by $kr << 1$ where r the distance between the source and the probe. This can be written as

$$r << \frac{\lambda}{2\pi} \tag{3}$$

which is typically the maximum distance to be considered in the near field region. Since the magnetic fields are more prominent in near field measurements, large magnetic probes are preferred.

Far-field: As opposed to the near field, the far field region is bounded by $kr >> 1$, which can be written as

$$r >> \frac{\lambda}{2\pi}. \tag{4}$$

This region is dominated by radiated fields where the electric and magnetic fields are orthogonal to each other. In far field measurements, both E and H fields can be measured and the larger amplitude of the field makes this measurement easier. A successful EM attack on a smart card from a far field distance of $\approx 5m$ has been performed in [2] In these experiments, a shielded environment requires only a few hundred measurements, which is comparable to a near field attack. Alternatively, in an unshielded environment, the number of required measurements may increase to a few thousand.

B. EM propagation

Electromagnetic emanations propagate from the source in four ways: i) electromagnetic radiation, ii) conduction, iii) modulation of another signal, and iv) acoustic signals [24]. Radiated EM emissions can be captured by using near field probes or antennas at a close proximity. If the amplitude is low, direct radiation should be measured in the near field. A cryptographic chip can be considered to contain multiple radiation sources in the form of current elements. Accordingly, a cryptographic chip is modeled by replacing small current loops with magnetic dipoles and common mode currents with electric dipoles in [25], considering their very similar field characteristics.

III. Threat model

A threat is defined as a situation or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service [27]. In our threat model, the targets are cryptographic circuits, which are running confidential information on the chip. The goal of the attacker is to learn information that s/he normally has no legitimate access to, *i.e.,* the secret keys. For the EM side channel attacks, the attacker typically needs inexpensive equipment such as a sensor or antenna, analog preprocessing equipment, analog to digital converter, and a cable connection. Many near field probes such as integrated inductors, hard disk heads, magnetic probes, and solenoids have been described in literature. The use of far field antennas like biconical antennas, discone antennas, and the folded dipole antennas have also been mentioned [23].

We assume that the secret keys are stored in the device and the attacker does not physically invade the device by de-capsulation or touching the chip with the probe. The attacker can achieve his goal without the need for finding or exploiting system flaws, but rather just running the normal process and performing legitimate operations. We also assume that an attacker has the device at his disposal, and is able to run it a number of times, possibly with input values of his choice. Additionally, during the processing, the attacker is able to extract the device's electromagnetic field pattern [29].

IV. On-chip power delivery

On-chip voltage regulation is an area with a vast amount of research activity to enable small, fast, efficient, robust, and high power-density voltage regulators on-die close to the load circuits [10], [13]. On-chip regulators provide faster voltage scaling, reduce the number of dedicated I/O pins, and facilitate fine-granularity power management techniques [10]–[12]. On-chip integration of voltage regulators increases complexity and consequently and can take significant design efforts. On-chip integration requires the same process technology as other chip components, making it difficult while maintaining high efficiency and system performance. The level of integration may also increase the chip size slightly [30]. Three types of regulators are widely used in modern circuits: buck converters (BC), switched-capacitor (SC) regulators, and linear regulators (LDO) [14], [26]. For a linear regulator, the dependency on the V_{OUT}/V_{IN} ratio has a negative impact on the power efficiency. Alternatively, switching regulators also exhibit challenges for on-chip implementation. Major drawback of this topology is the size of the inductor and capacitor that occupy large area [33]. Since the regulator is moved on-chip, the size of the filter components are reduced. Smaller filter components require higher switching frequencies, potentially reducing the power efficiency. Also, a smaller capacitor allows less charge transferred to the load per switching cycle [15].

IBM uses a distributed on-chip power delivery network in the POWER8 processor where the entire die has more than 750 ultra-small voltage regulators [31][1]. Intel utilizes a fully integrated voltage regulator (FIVR) architecture[2] to adaptively change the number of active phases within a buck converter based on the workload to maximize power efficiency over a wide current range [34].

One of the properties of distributed on-chip power delivery that is investigated in this paper is that the distance between the voltage regulator and load circuit (*i.e.,* cryptographic circuit) becomes significantly smaller. Alternatively, voltage regulators regulate the voltage at the point of load (*i.e.,* in close proximity to the load circuits). Since the current does not travel long distances, the regulated power can be distributed using semi-global and partly local power grid lines to minimize the voltage drop across the metal vias, as illustrated in Fig. 2. When the power is delivered through thinner metal lines at significantly closer distances, our hypothesis is that the EM emanations are expected to be significantly mitigated. There are three intuitive explanations: i) the amount of current would be significantly smaller, ii) the cross-section of the wires carrying current would be thinner, and iii) the local metal lines may be farther from the probe. In this paper, our hypothesis is validated with extensive HFSS simulations, as explained in Section V.

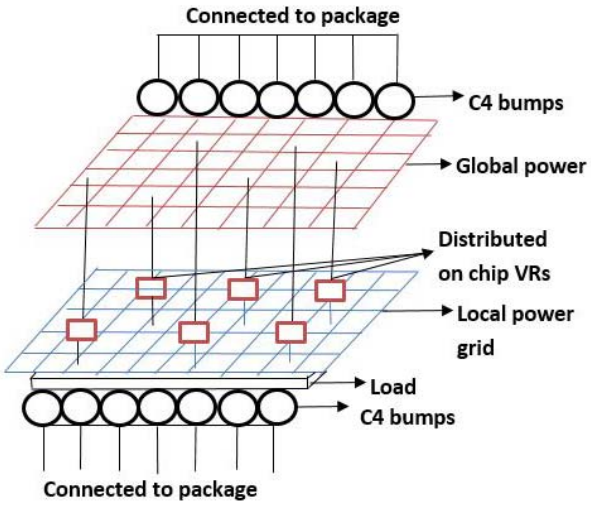

Figure 1. Distributed on-chip power delivery network.

A. Simulation setup

The implications of delivering power through the off-chip and on-chip voltage regulators on the amplitude of EM emissions are presented with extensive simulations in HFSS [35]. Driven Modal type simulation is selected in the HFSS to calculate the modal-based S parameters in terms of power. The S matrix solutions are expressed in terms of the incident and reflected powers of the waveguide modes. An excitation port permits energy to flow into and out of the structure. For this model, a lumped port is chosen as the excitation port. The local/global power grids are modeled based on the metal layer parameters in [36]. The solution frequency is chosen as 1 GHz. The frequency is swept from 400 MHz to 6 GHz with the step size of 0.1 GHz, where the rest of the data at intermediate frequencies are interpolated. The maximum number of adaptive passes allowed is 20 and the maximum change in the magnitude of S parameters between two consecutive passes (Delta S) is 0.02. The S parameters are plotted in the 2D Cartesian plane. The antenna used as a near field probe is a loop antenna with a circumference of 600 μm.

[1]IBM POWER8 has 12 chiplets and each chiplet has 64 voltage regulators

[2]FIVR is being used in Intel Haswell architecture.

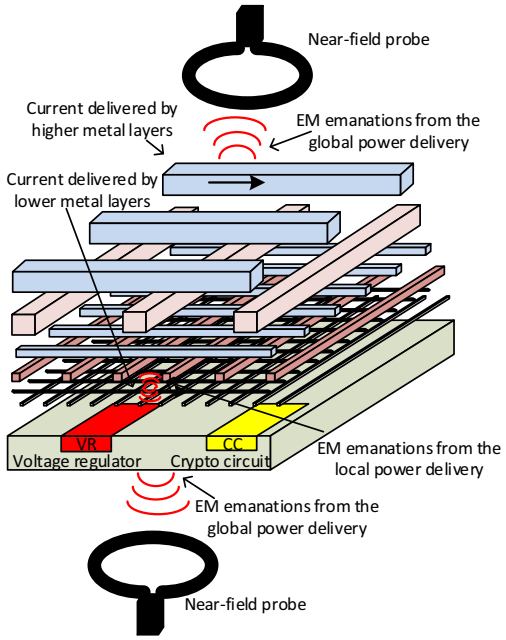

Figure 2. Leveraging local power delivery reduces EM emanations originating from the power delivery network.

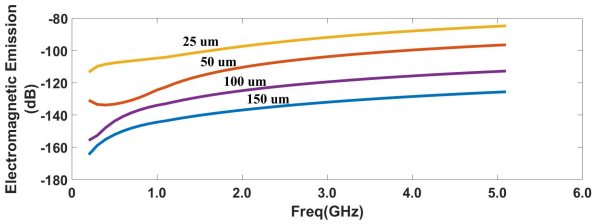

Figure 3. EM emissions from local grid at varying probe distances.

V. Evaluation

A. Effects of the size of the power grid and distance from the probe

While the highest two metal layers (eighth and ninth) are considered to form the global power grid, the lower metal layers (third and fourth) are considered to form the local power grid. We first analyze the emanations when a probe is placed at the top of the circuit. The emanations from the

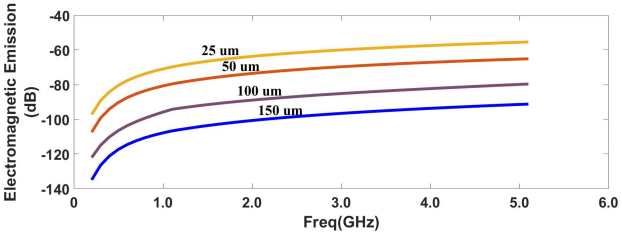

Figure 4. EM emissions from global grid at varying probe distances.

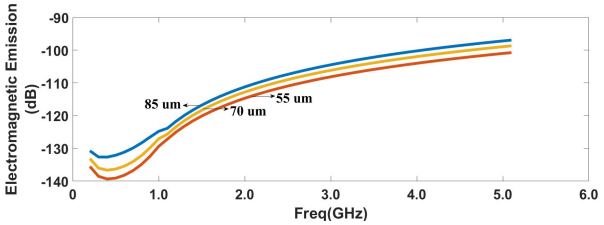

Figure 5. EM emissions from local grid for different wire lengths.

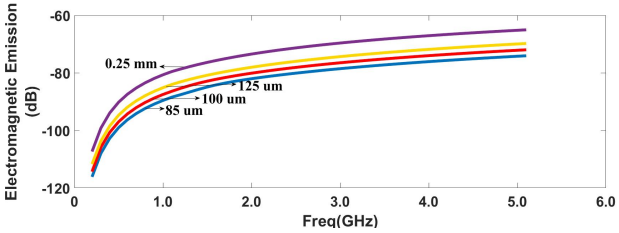

Figure 6. EM emissions from global grid for different wire lengths.

local and global power grid lines are extracted when the distance of the near field probe to the chip is swept from 25 μm to 150 μm, as shown respectively, in Figs. 3 and 4. The length of the local and global power grid lines are, respectively, 100 μm and 250 μm.

The amplitude of the EM emissions both from the global and local grids to the probe increases with frequency and with a reduction in the distance from the probe. The EM emanations from the global power grid lines are, however, more than 25 dB (up to 34 dB) greater than the EM emanations from the local power grid lines, as summarized in Table I.

Table I
EM Emanations from the local vs global power grids to a probe placed at varying distances.

Distance from probe	Local Grid	Global Grid
25 um	-104.4053 dB	-70.4994 dB
50 um	-122.6810 dB	-79.5490 dB
100 um	-132.9984 dB	-95.3681 dB
150 um	-144.0217 dB	-108.4753 dB

The primary reason is that the thinner interconnect wires cause lower EM emanations as compared to the thicker global lines. Next, the EM emanations from the local and global power grid lines with various lengths have been simulated.

For the same probe distance of 50 μm, the EM emanations from the local grid are reduced by almost 40 dB as compared to the global grids, as seen from Figs. 5 and 6, due to shorter wire lengths. For the same interconnect length of 85 um, the emission from the local grid is almost 35 dB lower than the emanations from the global grid due to thinner dimensions of the wires. Typically, the length of the global interconnect is roughly equivalent to the size of the die (1-2 mm). As seen from Table II, even for an interconnect length of 0.25 mm,

Table II
EM EMANATIONS FROM THE LOCAL AND GLOBAL POWER GRIDS TO A PROBE FOR DIFFERENT WIRE LENGTHS.

Length of wire(um)	Local Grid Emission(dB)	Global Grid Emission (dB)
55 um	-127.1706	-
70um	-125.6433	-
85 um	-123.8549	-88.4574
100 um	-	-86.4093
125 um	-	-84.0472
250 um(0.25 mm)	-	-79.5490

the EM emission is approximately -79.5490 dB, which is significantly larger than that from the local grid lines which are of much smaller lengths.

So far, we assumed that the attack is performed from the top of the chip as the signal strength in this case is significantly higher and the attacker would require less post processing elaboration. To verify this assumption the probe is moved to the bottom of the chip to capture and compare the electromagnetic traces. The probe is placed at a distance of 100 μm from both the local and global interconnects. The captured EM emanations are shown in Fig. 9, which confirms the above mentioned hypothesis. When capturing the EM emanations from the bottom, there is a decrease of 8 dB in emissions from global interconnect wires. The increased distance and shielding from the substrate are the two main reasons for this reduction. The emissions from the local wires, however, are increased. This is because the probe is now relatively closer to the wires as compared to the case when the probe was placed at the top of the chip. The emanations from the global wires can still be seen to be higher than the emanations from the local wires, which supports our claim that on chip regulation may significantly improve the security. The comparison can also be seen in Table III, for the interconnect length of 100 μm, the EM emission from global grid is -103.4635 dB, which is significantly higher than that of the local grid of the same length.

Table III
EM EMANATIONS FROM THE LOCAL AND GLOBAL POWER GRIDS TO A PROBE PLACED AT 100 UM.

Probe Position	Local Grid	Global Grid
Top	-132.9984 dB	-95.3681 dB
Bottom	-114.6810 dB	-103.4635 dB

B. Security implication

The security implications as a function of the signal strength are explained in this section This section validates our discussion with mathematical calculations performed under the same scenarios stated in the previous sections. Assuming that PS_1 is the power of the EM signal without the proposed countermeasure, P_N is the measured power noise,

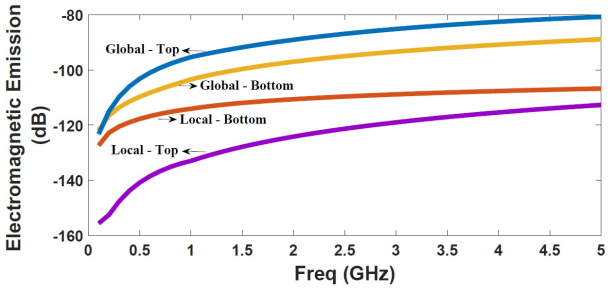

Figure 7. EM emissions comparison of local and global grids at 100 um.

and P_S is the power of the signal with countermeasure,

$$10Log\frac{PS_1}{P_N} - 10Log\frac{PS_2}{P_N} = 33 \tag{5}$$

$$\frac{PS_1}{PS_2} = 1995. \tag{6}$$

Signal to noise ratio (SNR) is a measure of how much useful information is present in a system.

$$SNR_1 = Var\frac{PS_1}{P_N} \quad with\ countermeasure \tag{7}$$

$$SNR_2 = Var\frac{PS_2}{P_N} \quad without\ countermeasure \tag{8}$$

$$SNR_2 = SNR_1\frac{Var(PS_2)}{Var(PS_1)} = SNR\frac{1}{1995}. \tag{9}$$

The relation between the SNR and the correlation coefficient can be written as

$$Correlation\ y = \frac{1}{\sqrt{1+SNR}} \tag{10}$$

The number of plaintexts required to perform a correlation analysis attack with a success rate of 0.9 $N_{0.9}$ can be estimated with [37]

$$N_{0.9} \approx C \times \frac{1}{y^2} = C(1+\frac{1}{SNR_2}) \tag{11}$$

$$\approx \frac{C}{SNR_2} = \frac{C}{SNR_1} \times (1995)^2 \tag{12}$$

where c is a constant depending on the number of key guesses considered and the required success rate. The enhancement in the measurement to disclosure (MTD) value comes out to be $(1995)^2$ which is considered a significant improvement. Similarly, from Table 3, the EM emanations from the global interconnect is approximately 11 dB higher than the emanations captured from the local grid. Using this result and following the same procedure as

$$10Log\frac{PS_1}{PS_2} = 11 \tag{13}$$

$$N_{0.9} \approx C \times \frac{1}{y^2} = \frac{C}{SNR_1} \times (13)^2. \tag{14}$$

The MTD enhancement ratio does not decrease significantly if the attack is performed from the bottom. This is primarily

because when captured from the bottom, the EM emanations by the global grid is decreased but increased by the local grid, due to the close proximity to the measuring probe.

While the MTD enhancement ratio is significantly larger for the attacks that are performed from the top side, the EM signal strength is still larger when the attack is performed from the top side as compared to the bottom side. Using on-chip voltage regulators, EM emissions from the top can be reduced by 33 dB and the MTD enhancement ratio is increased by a factor of $(1995)^2$. Likewise we observe a reduction of 11 dB in EM emissions and an increase in the MTD enhancement ratio by a factor of $(13)^2$ from the bottom. In the following sections, two techniques are discussed to further reduce the EM emissions from the top probe, making the attack even more difficult to perform.

C. Shielding with MIM capacitors

Sheet metal is typically used for shielding EM radiation. Copper absorbs radio and magnetic waves and is used for RF shielding [38]. The electric field in EM radiation produces forces on the electrons in the conductor, which causes displacement of charges inside the conductor and cancels the applied field. Similarly, magnetic fields produce eddy currents inside the conductor which reflect the electromagnetic radiation from the surface.

However, due to the electrical resistivity of the conductor, the excited field does not completely cancel the applied field. Any holes in the shield must be significantly smaller than the wavelength of the radiation that is trying to be kept out. Holes bigger than the wavelength allow the current to flow around them so the incident wave does not excite the opposing electromagnetic fields [39]. High frequencies (100 MHz-40 GHz) are extremely sensitive to gaps in the shielding enclosure. Also, due to the ferromagnetic response of the conductors to low frequency magnetic field, these fields are not completely mitigated by the conductor [39]. All these factors reduce the shielding capability of a conductor [39].

EM shielding also occurs due to absorption. The loss due to absorption is proportional to the thickness of the shield, and is because of the presence of electric or magnetic dipoles, which interact with the fields in the incident radiation. Shielding can also occur due to multiple reflections from the conductor surface. The loss due to multiple reflections is directly related to the surface area of the shield where a larger interface area increases the radiation loss. At higher frequencies, electromagnetic radiation penetrates only the near surface of an electrical conductor which is known as skin effect [40].

Two metal-layer MIM capacitors are widely utilized in CMOS processes. With the parallel-plate structure, the MIM capacitor is composed of two metal plates and a dielectric layer between them. The fabrication of MIM capacitor needs additional fabrication masks to define the top and bottom

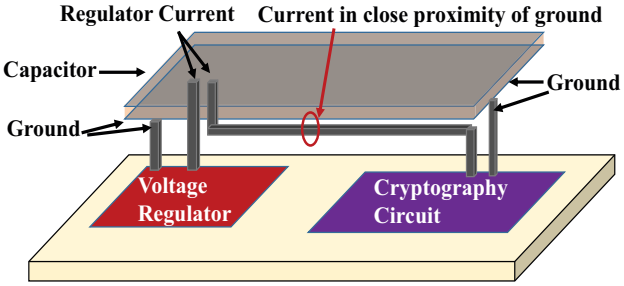

Figure 8. Using MIM capacitor as a shield.

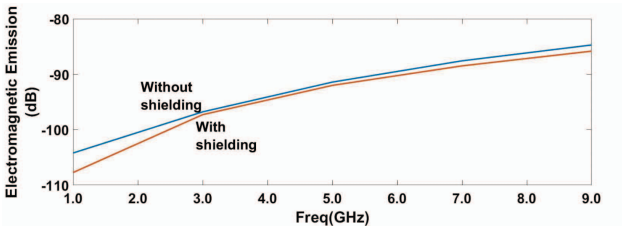

Figure 9. Reduction in EM emission due to shielding effect of the MIM capacitor.

metal plates that increase the cost of production [41]. We experimented with MIM capacitors and investigated the effectiveness of MIM capacitors on minimizing the EM emanations from the local power grids, as illustrated in Fig. 8. MIM capacitors are typically implemented between the fifth and sixth metal layers, making them physically appropriate to shield the local power grid lines which use the third and fourth metal layers in our simulations. Fig. 9 depicts the effect of using an MIM capacitor to shield the local power grid. As tabulated in Table IV, the MIM shielding leads to a reduction in the EM emission by almost 3 dB at the solution frequency of 1 GHz. The MIM shielding therefore does not significantly reduce the EM emanations from the local power grid lines.

The primary reason is that the MIM shield, while blocking some of the radiation, may boost the emanations by creating a certain amount of current due to the inductive coupling from the local power grid. The generated inductive current therefore negates the shielding effects of the MIM capacitors.

D. Effect of upper metal layers on the EM emanations from lower metal layers

The effects of higher metal layers on the EM emanations from the lower metal layers to a probe are investigated. As shown in Fig. 10, due to the inductive coupling

Table IV
EM COMPARISON WITH MIM SHIELDING.

Solution Frequency (GHz)	EM without shielding(dB)	EM with shielding (dB)
1	-104.4053	-107.7182

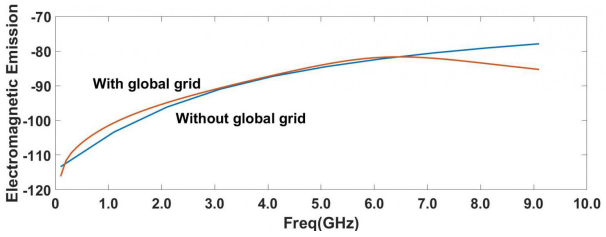

Figure 10. Effect of the global grid on the emanations from the local power grid.

Table V
EM COMPARISON WITH MIM SHIELDING.

Solution Frequency (GHz)	EM without upper metal layer(dB)	EM with upper metal layer (dB)
1	-104.4053	-101.4948

between the different metal layers located close to each other, the EM radiation emitted by the lower metal layer increases by a small amount($\sim$2.7 dB) at the solution frequency of 1 GHz, as shown in Table V. Due to the presence of the gaps in the upper metal layers, which are almost as large as the wavelength of the incoming radiation, the upper layers do not act as an effective shield and fail in attenuating the incident radiation. Instead, because of the magnetic field generated in the lower layer, a small current is induced in the upper layer, which further generates an additional electromagnetic field that is coupled with the one generated by the lower metal layer. As a result, the upper metal layers, if no intentional current is flowing, would even boost the EM emanations from the local power grids by a small amount (*i.e.* $\sim$2.7 dB).

VI. DISCUSSION

The primary issue of delivering power through the local interconnect lines is the increased impedance of the local interconnect as their cross-sectional area is lower than that of the global power interconnect lines. The physical distance from a local voltage regulator to a load circuit is significantly reduced as compared to the distance from an off-chip regulator to an on-chip load circuit. Additionally, the power provided by an off-chip voltage regulator also needs to go through the package and/or board level interconnects as well as the pad/pin parasitic impedance. As compared to passing through all of these parasitic impedances, the output power of a localized on-chip voltage regulator only needs to travel small distances. Considering these differences between the off-chip voltage regulators and distributed on-chip voltage regulators, delivering the required power through lower metal lines to the circuits at close proximity would not cause significant amount of noise [15]. Additionally, the power output of each individual distributed voltage regulator is significantly smaller than that of the off-chip regulators, making it possible for the localized regulated power to be delivered through the local power grid lines.

VII. CONCLUSION

In this paper, the implications of distributed on-chip power delivery on EM side channel attacks are investigated. The key idea is the observation that on-chip voltage regulators can utilize shorter and thinner local interconnect wires, and the EM emissions from the circuit would be considerably lower than those from circuits using off-chip voltage regulators which have to utilize thicker global wires. A 33 and 11 dB reduction in the EM emanations from top and bottom can be achieved, respectively, when distributed on-chip voltage regulators are utilized instead of off-chip voltage regulators. In the analysis, we are able to simulate global grid up to 0.25 mm length due to computational complexity of the simulation with longer wires. With typical global grids having lengths of 1-2 mm, the EM radiation is significantly higher than local grids when captured from either top or bottom. We also demonstrate that shielding a cryptographic circuit with MIM capacitors can further decrease the emission of EM side channel information by less than 3 dB.

VIII. ACKNOWLEDGEMENT

This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451 and by a Cisco Systems Research Award.

REFERENCES

[1] P. Kocher, J. Jaffe and B. Jun, *Differential Power Analysis,* Springer, 1999.

[2] S. Mangard, E. Oswald and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards,* Springer Science, 2008.

[3] W. Yu, O. A. Uzun and S. Köse, "Leveraging On-Chip Voltage Regulators as a Countermeasure Against Side-Channel Attacks," *Proceedings of the IEEE/ACM Design Automation Conference (DAC)*, pp. 1 - 6, June 2015.

[4] W. Yu and S. Köse, "A Lightweight AES Implementation Against Bivariate First-Order DPA Attacks," *Proceedings of the ACM Workshop on Hardware and Architectural Support for Security and Privacy (HASP)*, pp. 1 - 7, June 2017.

[5] K. Boris and B. David, "An Information-theoretic Model for Adaptive Side-channel Attacks," *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 286-296, July 2007.

[6] E. Brier and M. Joye, "Weierstras Elliptic Curves and Side-channel Attacks," *Springer*, Vol. 2274, pp. 335-345, May 2002.

[7] J. J. Quisquater and D. Samyde, "Electro-Magnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards," *Smart Card Programming and Security*, Vol. 40, pp. 200-210, November 2001.

[8] D. Agrawal, B. Archambeault, R. Rao and P. Rohatgi, "The EM Side-Channel(s)," *Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems Springer*, Vol. 2523, pp. 29-45, February 2003.

[9] W. Yu and S. Köse, "A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks,'" *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 63, No. 8, pp. 1152 - 1163, August 2016.

[10] S. Köse, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, "Active Filter Based Hybrid On-Chip DC-DC Converters for Point-of-Load Voltage Regulation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 48, No. 2, pp. 587 - 597, February 2013.

[11] S. Köse and E. G. Friedman, "An Area Efficient Fully Monolithic Hybrid Voltage Regulator," *Proceedings of the IEEE International Symposium on Circuits and Systems*, pp. 2718 - 2721, May 2010.

[12] S. K. Khatamifard, L. Wang, W. Yu, S. Köse, and U. R. Karpuzcu, "ThermoGater: Thermally-Aware On-Chip Voltage Regulation," *Proceedings of the IEEE International Symposium on Computer Architecture (ISCA)*, pp. 120 - 132, June 2017.

[13] L. Wang, S. K. Khatamifard, O. A. Uzun, U. R. Karpuzcu, and S. Köse, "Efficiency, Stability, and Reliability Implications of Unbalanced Current Sharing among Distributed On-Chip Voltage Regulators," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*,Vol. PP, No. 99, pp. 1 - 14, 2017.

[14] O. A. Uzun and S. Köse, "Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 4, No. 2, pp. 169 - 179, June 2014.

[15] S. Köse, and E. G. Friedman, "Distributed On-chip Power Delivery," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 2, No. 4, pp. 704-713, December 2012.

[16] W. Yu and S. Köse, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," *IEEE Transactions on Emerging Topics in Computing*, Vol. PP, No. 99, pp. 1 - 1, October 2016.

[17] W. Kim, S. Gupta, G. Wei and D. Brooks, "System Level Analysis of Fast, Per-core DVFS using On-chip Switching Regulators," *Proceedings of the IEEE International Symposium on High Performance Computer Architecture,* pp. 123-134, February 2008.

[18] K. Chava and J. Silva-Martinez, "A Frequency Compensation Scheme for LDO Voltage Regulators," *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 51, No. 6, pp. 1041-1050, September 2004.

[19] R. J. Milliken, J. Silva-Martinez and S. Sinencio, "Full On-Chip CMOS Low-Dropout Voltage Regulator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 54, No. 9, pp. 1879-1890, September 2007.

[20] R. Callan, A. Zajić and M. Prvulovic, "FASE: Finding Amplitude-Modulated Side-Channel Emanations," *ACM SIGARCH Computer Architecture News*, Vol. 43, No. 3, pp. 592-603, June 2015.

[21] P.T. Pappas, "The Original Ampere Force and Biot-Savart and Lorentz Forces," *Il Nuovo Cimento B*, Vol. 76, No. 2, pp. 189-197, August 1983.

[22] A. Zajic and M. Prvulovic, "Experimental Demonstration of Electromagnetic Information Leakage from Modern Processor Memory Systems," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 56, No. 4, pp. 885-893, August 2014.

[23] D. Mulder, "Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices," *Diss. PhD Thesis*, KU Leuven, July 2010.

[24] National Security Agency, "NACSIM 5000: TEMPEST Fundamentals," February 1982.

[25] A.S. Machado, *Low-Power HF Microelectronics: A Unified Approach,* IEEE Press, March 1996.

[26] C. F. Lee and P. K. Mok, "A Monolithic Current-Mode CMOS DC-DC Converter with On-Chip Current-Sensing Technique," *IEEE Journal of Solid-State Circuits*, Vol. 39, No. 1, pp. 3-14, January 2004.

[27] C. Rechberger and E. Oswald, "Stream Ciphers and Side-Channel Analysis," *In ECRYPT Workshop, SASC-The State of the Art of Stream Ciphers*, pp. 320-326, October 2004.

[28] J. Guo and K. N. Leung, "A 6-μW Chip-Area-Efficient Output-Capacitorless LDO in 90-nm CMOS Technology," *IEEE Journal of Solid-State Circuits*, Vol. 45, No. 9, pp. 1896-1905, September 2010.

[29] A. Aldini, R. Gorrieri and F. Martinelli, Foundations of Security Analysis and Design III: FOSAD 2004/2005 Tutorial Lectures, *Springer-Verlag*, 2005.

[30] B. Schweber, 'Understanding the Advantages and Disadvantages of Linear Regulators," Available: [Online] *https://www.digikey.com/en/articles/techzone/2012*, August 2012.

[31] E. J. Fluhr and Others "The 12-Core POWER8 Processor With 7.6 Tb/s IO Bandwidth, Integrated Voltage Regulation, and Resonant Clocking," *IEEE Journal of Solid-State Circuits*, Vol. 50, No. 1, pp. 10-23, January 2015.

[32] S. Lai and P. Li, "A Fully On-Chip Area-Efficient CMOS Low-Dropout Regulator with Fast Load Regulation," *Analog Integrated Circuits and Signal Processing*, Vol. 72, No. 2, pp. 433-450, August 2012.

[33] W. Kim, M. S. Gupta, G. Wei and D. M. Brooks, "Enabling On-chip Switching Regulators for Multi-core Processors Using Current Staggering," *In Proceedings of the Work on Architectural Support for Gigascale Integration*, August 2007.

[34] E. A. Burton and Others "FIVR - Fully Integrated Voltage Regulators on 4^{th} Generation Intel Core SoCs," *Applied Power Electronics Conference and Exposition (APEC)*, pp. 432-439, March 2014.

[35] Ansoft, HFSS, Version 11, *Ansoft Corporation, Pittsburgh, PA*, 2007.

[36] K. Mistry and Others "A 45nm Logic Technology with High-k+Metal Gate Transistors, Strained Silicon, 9 Cu Interconnect Layers, 193nm Dry Patterning, and Pb-free Packaging," *IEEE International Electron Devices Meeting*, Vol. 2, pp. 247-250, May 2007.

[37] O. X. Standaert, E. Peeters, G. Rouvroy and J. J. Quisquater, "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," *Proceedings of the IEEE*, Vol. 94, No. 2, pp. 383-394, February 2006.

[38] P. F. Lilienthal II and V. F. William, "Circuit Board RF Shielding," *US Patent 6,239,359*, May 2001.

[39] "Practical EM Shielding by Learn-EMC," Available : [Online] *http://learnemc.com/practical-em-shielding*, 2016.

[40] D. C. Mattis, and J. Bardeen, "Theory of the Anomalous Skin Effect in Normal and Superconducting Metals," *Physical Review*, Vol. 111, No.2, pp. 412-417, February 1958.

[41] C. Po-Yen and K. Ming-Dou, "Metal-layer Capacitors in the 65nm CMOS Process and the Application for Low-Leakage Power-Rail ESD Clamp Circuit," *Microelectronics Reliability*, Vol. 54, No. 1, pp. 64-70, August 2013.