Killing EM Side-Channel Leakage at its Source

Invited Paper

Debayan Das[1], Mayukh Nath[1], Santosh Ghosh[2], Shreyas Sen[1]
[1]*School of Electrical and Computer Engineering, Purdue University, USA*
[2]*Intel Labs, Hillsboro, Oregon, USA*
{*das60, nathm, shreyas*}*@purdue.edu, santosh.ghosh@intel.com*

***Abstract*—Side-channel analysis (SCA) is a big threat to the security of connected embedded devices. Over the last few years, physical non-invasive SCA attacks utilizing the electromagnetic (EM) radiation (EM side-channel 'leakage') from a crypto IC has gained huge momentum owing to the availability of the low-cost EM probes and development of the deep-learning (DL) based profiling attacks. In this paper, our goal is to understand the source of the EM leakage by analyzing a white-box modeling of the EM leakage from the crypto IC, leading towards a low-overhead generic countermeasure. To kill this EM leakage from its source, the solution utilizes a signature attenuation hardware (SAH) encapsulating the crypto core locally within the lower metal layers such that the critical correlated crypto current signature is significantly attenuated before it passes through the higher metal layers to connect to the external pin. The protection circuit utilizing AES256 as the crypto core is fabricated in 65nm process and shows for the first time the effects of metal routing on the EM leakage. The $> 350\times$ signature attenuation of the SAH together with the local lower metal routing ensured that the protected AES remains secure even after $1B$ measurements for both EM and power SCA, which is an $100\times$ improvement over the state-of-the-art with comparable overheads. Overall, with the combination of the 2 techniques - signature suppression and local lower metal routing, we are able to kill the EM side-channel leakage at its source such that the correlated signature is not passed through the top-level metals, MIM capacitors, or on-board inductors, which are the primary sources of EM leakage, thereby preventing EM SCA attacks.**

***Index Terms*—EM Side-channel attack, Low-overhead countermeasure, White-box modeling, Signature Suppression, Local lower metal routing.**

I. Introduction

Electromagnetic (EM) side-channel analysis (SCA) attacks are becoming increasingly threatening with the development of low-cost EM probes. Moreover, the increasing growth of the internet-connected embedded devices makes the attack space larger than ever before. To address the concerns of the security and confidentiality of data, most embedded devices today employ cryptographic algorithms, which are computationally secure. However, as these algorithms are implemented on a physical substrate, they leak critical information in the form of EM radiation, power consumption, timing, cache hits and misses, and so on, which can be picked up by an interested adversary to obtain the secret key operating in the device. In this article, we focus on the hardware SCA attacks, specifically the non-invasive EM SCA attacks.

This work was supported in part by the National Science Foundation (NSF) under Grants CNS 17-19235, CNS 19-35573, and in part by Intel Corporation.

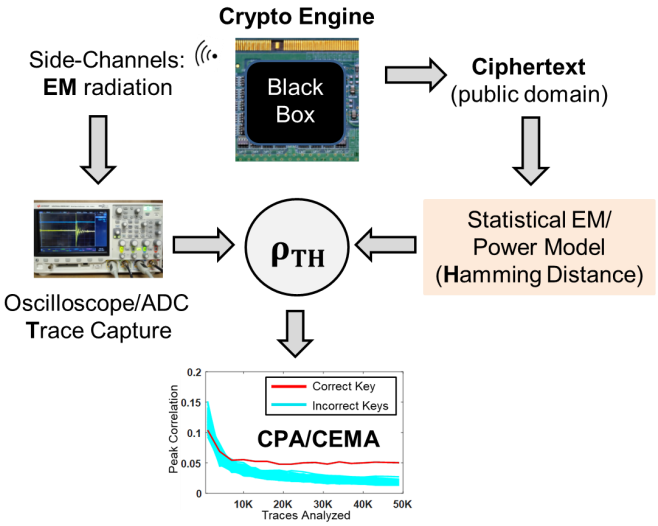

Fig. 1. Overview of EM SCA attack and set-up. Most existing works treat the EM emanation as a black-box without paying much attention to the cause of the EM leakage. This work provides a white-box approach to analyze the root-cause of this EM leakage.

II. EM SCA Background & White-box Analysis

A. Preliminaries

In classical cryptography, the notion of security is derived from mathematical abstractions, and revolves around the concepts of one-way and trapdoor functions. One-wayness implies that the function is easy to compute but hard to invert. A trapdoor one-way function is easily invertible only in presence of the secret 'key'. Classical cryptanalysis of prominent cryptographic protocols like the AES128/SHA256 shows high resilience against brute-force attacks. However, over the last two decades, many of the security protocols have been attacked using EM or power SCA attacks by taking advantage of the underlying physical implementation to recover secret parameters like the key [1], [2], [3].

For an EM SCA attack, as shown in Fig. 1, the attacker captures a set of EM 'traces' using an EM probe (H-field/E-field probe) during the encryption operation of the target device. Once the traces are collected, the attacker can mount a correlation/differential EM attack (CEMA/DEMA) to recover the secret key [4], breaking one key byte at a time (for AES). In case of CEMA, the captured traces are correlated across

978-1-7281-8058-8/20/$31.00 ©2020 IEEE

a hamming weight (HW) or a hamming distance (HD) model built for each key byte with known ciphertexts (more practical scenario) or chosen plaintexts. After analyzing multiple traces, the correct key byte showing the maximum correlation separates out from the other 255 bytes and is thereby recovered. Performing the process for all the 16 key bytes reveals the entire secret key of AES128 [5].

B. Why do we care?

Transitioning from AES128 to AES256, the mathematical security is enhanced exponentially while the SCA resilience is only increased linearly by a factor of 2×. Recently, EM SCA attacks on the AES256 engine have been demonstrated within 5 minutes even from a distance of 1 meter using only $200 equipment [6]. A major advantage of EM SCA over the power attack is that it is non-invasive [7] and many remote attacks have already been demonstrated [8], [9]. Recently, a low-cost end-to-end automated EM SCA attack have been demonstrated using the *SCNIFFER* framework [10]. It utilizes a 3D printer as the EM scanner to scan an embedded device to extract the secret key efficiently using a greedy gradient search heuristic algorithm. Such platforms show the vulnerability of today's embedded systems, specifically devices utilizing fixed key implementations. More real-world EM/power SCA attacks include the KeeLoq keyless entry systems [11], Atmel CryptoMemory authentication [12], Xilinx FPGA bitsream encryption [13], cryptocurrency wallets [2], [14].

EM SCA uses the radiated EM fields to extract the secret keys. Similar EM field leakages can be exploited to perform EM attacks on critical on-body devices like the pacemakers or insulin pumps, which if hacked could prove lethal. To prevent such electromagnetic attacks on wearable devices, recently electro-quasistatic human body communication (EQS-HBC) has been proposed as a promising alternative to the traditional radiative wireless body area networks (WBAN), as EQS-HBC can confine the critical signals within the human body without unncessarily radiating the signals outside, enabling a covert body area network and providing the physical security [15], [16]. Also, recently, screaming attacks [17] have been shown which exploits the radiative property of wireless communication (critical digital signals modulated on top of the analog radio components) to break the security of a mixed-signal design from a long distance. The EM side-channels can also be utilized for malware detection [18].

Other than the correlational/differential EM SCA, which are direct non-profiled attacks, profiling EM SCA attacks has evolved recently. Continuous works in the domain of machine-learning based profiled EM/power SCA attacks [19], specifically deep-learning (DL) attacks [20], have been promising. These profiling attacks are much more powerful compared to the traditional CEMA/DEMA attacks. DL SCA attacks occur in two phases - profiling phase and the attack phase. During the profiling phase, a deep neural network (DNN) model is trained with multiple traces and the corresponding keys. After the offline training is done, a cross-device attack on an unseen device of the same architecture can be mounted with as low as a single

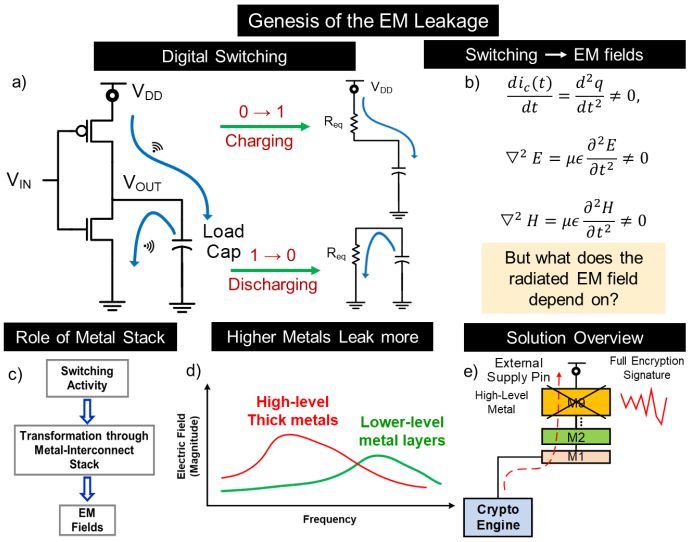

Fig. 2. Genesis of the EM Leakage: (a) Switching of the digital gates creates changing electric fields which in turn produces magnetic fields according to the Maxwell's equations (b), leading to EM radiation. However, we need to understand what these EM fields really depend on. (c) Switching currents flowing through the metal-interconnect stack undergoes a transformation to create this EM radiation and the magnitude of the fields depend on the dimensions of the metal layers. (d) Higher level metals are thicker, and has lower resonance freq. and hence the EM leakage from these top metals has higher probability of detection using commercially available EM probes. (e) Hence, the goal is not to pass the correlated crypto signature through the higher-level metal layers.

trace [21]. These cross-device single-trace DL SCA attacks are made even more efficient through a combination of (a) multi-device training, (b) principal component analysis (PCA) to identify the most significant dimensions and generalize the DNN model, and (c) dynamic time warping (DTW) to time-align power/EM traces before feeding to the fully connected DNN [22]. These DL SCA based attacks increase the threat surface of the embedded devices significantly as an attacker can carry out the attack using only single or few traces, thereby decreasing the time for access to the device.

Despite all these advancements, it needs to be noted that most works till date, both attacks and countermeasures, treat the crypto engine as a black box. Common countermeasures against EM SCA attacks include data randomization with noise injection, which has significantly high power overheads. EM shielding using Faraday cage is not a feasible solution since the pins need to connect to the external world. Masking has been studied as an effective countermeasure, but it has high area and power overheads and is also algorithm specific. Hence, in order to develop an efficient countermeasure, it is extremely important to understand the root-cause of this EM leakage and perform a white-box modeling of the EM from an integrated circuit.

C. Why does the EM leak information?

Cryptographic engines like AES/SHA/ECC consists of multiple digital gates. As the outputs of these digital gates switch their states, the acceleration of the electrons create changing

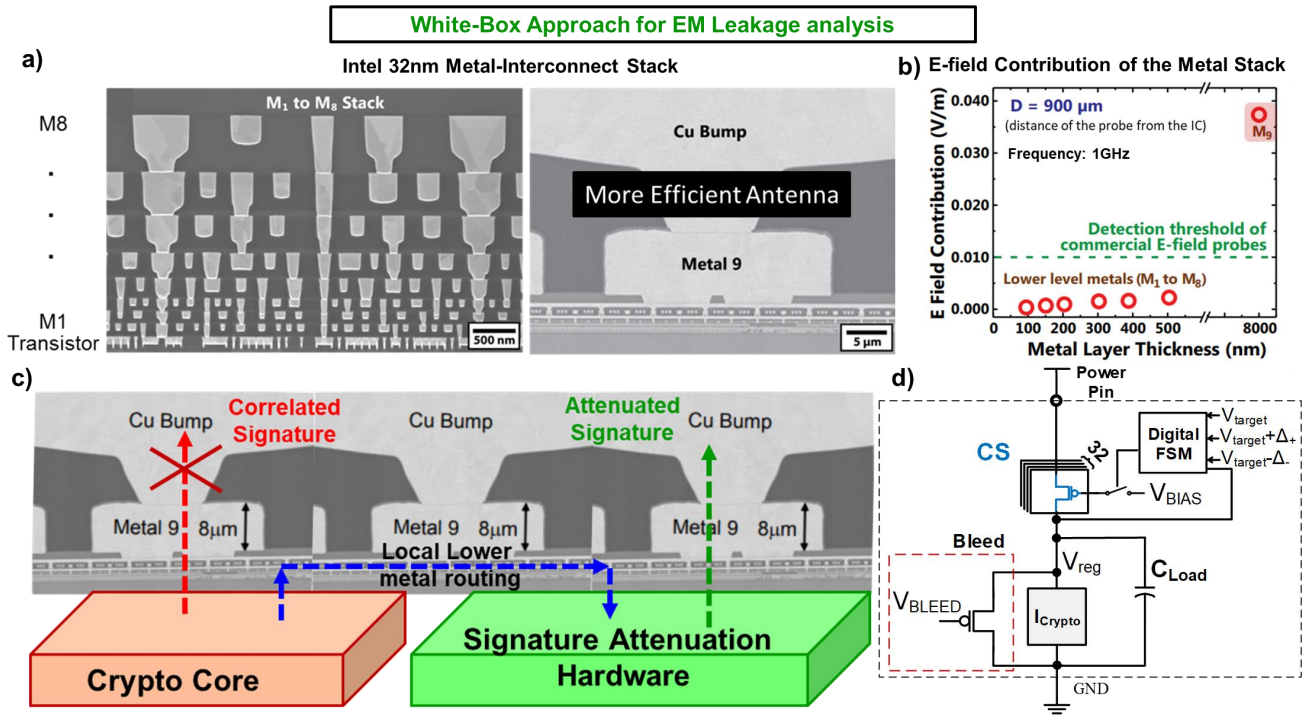

Fig. 3. White-box Modeling and analysis: (a) Intel 32nm metal-interconnect stack. (b) E-field contribution of the individual metal layers using HFSS shows that the EM leakage from the higher metal layers is detectable using commericially-available EM probes, (c) EM SCA Countermeasure: The crypto core is routed within the lower metals and then embedded locally using a SAH (also routed in lower metals) which significantly suppresses the correlated critical signature before passing it through the top metal layers. (d) SAH Circuit design.

electric fields which in turn produces magnetic fields, leading to EM radiation, according to the Maxwell's equations (Fig. 2(a, b)). But what does the magnitude of the radiated fields depend on? Well, it is the metal layers inside the IC carrying the current, which behave as antennas and radiate. Now, these switching currents passing through the metal layers undergo a transformation to create EM radiation and the magnitude of the generated fields depend on the dimensions of the metal layers (Fig. 2(c)). Higher-level metals are thicker and has lower resonance frequency, and hence the EM leakage from these top metals has a higher probability of detection using the commercially available EM probes [23] (Fig. 2(d)). Hence, our goal is not to pass the correlated crypto current through the top metal layers (Fig. 2(e)). But, how can we achieve that?

D. White-Box Analysis: How to stop the EM Leakage?

Now, we need to better understand the root-cause of the EM leakage, and hence a white-box modeling is necessary. Let us consider an Intel 32nm metal-interconnect stack as shown in Fig. 3(a). We can see that as we go up the metal stack, the higher-level metals are thicker and these higher metals M_9 and the copper bump are huge compared to the lower metal layers. Using 3-D high frequency structure simulator (HFSS), we see that, for the Intel 32nm technology, EM radiation from metals M_9 and above can be detectable using the commercially available EM probes (Fig. 3(b)). Hence, we need to ensure that the critical current signature is not passed through the higher metal layers. Sensitive signals can be routed within the lower metal layers. But power has to come from the off-chip components and hence needs to connect to the external pins through the higher metal layers. So, how can we restrict the correlated power signature to the lower metal layers?

Let us look into the state-of-the art circuit-level EM/power SCA countermeasures. It includes switched capacitors [24], integrated voltage regulators (IVRs) [25], and series LDOs [26]. Switched capacitor based current equalization circuit has multiple trade-offs, leading to a 2× throughput degradation. IVRs and series LDOs use large passives including MIM (metal-insulator-metal) capacitors utilizing the higher level metals which radiate leading to EM leakage. All these countermeasures have thus treated the EM leakage as a black box leading towards high overhead implementations.

III. SAH with Lower-Level Metal Routing

A. Local Lower Metal Routing

To realize our goal of not passing the critical signature through the higher metals, we propose routing the crypto core locally within the lower metal layers utilizing a signature attenuation hardware (SAH) which suppresses the critical signature significantly, before it reaches the top level metal layers (Fig. 3(c)). With the SAH embedding the crypto core within the lower metals, the attenuated signature passes through the higher metals, thereby ensuring that the EM leakage is significantly reduced and is not detectable using the commercial EM probes.

B. Signature Attenuation Hardware

The design of the SAH is shown in Fig. 3(d). The idea is to suppress the correlated current signature significantly before it reaches the power supply pin. Ideally, our goal is to have a constant supply current, such that it is independent of the crypto current. The closest is a constant current source (CS), which is realized using a biased PMOS stage [27]. A low-bandwidth switched mode control (SMC) loop operates at the start-up to choose the number of CS stages to turn ON depending on the average crypto current. It also compensates for any process/voltage/temperature (PVT) variations, and remains disengaged in steady state [28]. The shunt PMOS bleed provides a local negative feedback and allows DC regulation. The signature attenuation is given by the load capacitor and the output impedance of the top CS in saturation.

C. Combined effect & Results

The SAH embeds the crypto core locally within the lower metal layers to protect against both EM as well as power SCA attacks. The choice of the lower metal layer to which the SAH is routed up to, depends on the particular technology, and the IR drop tolerable across the crypto core.

The countermeasure circuit is fabricated using a 65nm test chip with a parallel AES256 as the crypto core [28]. Measurement results showed a $350\times$ signature attenuation provided by the SAH. With the protected implementation with higher-level metal routing, test vector leakage analysis (TVLA) was much higher than the protected implementation with lower metal routing, proving for the first time the effects of metal routing on the EM SCA leakage using on-chip measurements. The protected implementation is also resilient against the DL SCA attacks, showing that the deep neural network could not be trained even after $10M$ measurements [29], while it learnt the leakage patterns with $< 5K$ traces for the unprotected AES256. Overall, the proposed countermeasure achieved $100\times$ improvement in the minimum traces to disclosure (MTD) than the state-of-the-art countermeasures ($> 1B$) for both EM as well as power SCA using signature attenuation and local lower-level metal routing, with comparable overheads compared to the existing countermeasures.

IV. Conclusion

This work presents the first white-box modeling of the EM leakage from a crypto hardware, which leads to the understanding that the critical correlated signature should not be passed through the higher metal layers. To achieve this goal, a signature attenuation hardware (SAH) is utilized, embedding the crypto core locally within the lower metal layers so that the critical signature is not passed through the higher metals, which behave as efficient antennas and its radiation can be picked up by a nearby attacker. Measurement results from the 65nm testchip shows $> 350\times$ signature attenuation, leading to $100\times$ MTD improvement over the prior works. Also, the effect of metal routing on the EM SCA was demonstrated using TVLA showing that local lower-level metal routing plays a crucial role to prevent EM SCA attacks. Finally, to summarize, the combination of the 2 techniques - signature suppression and local lower metal routing kills the EM side-channel leakage at the source itself so that the correlated crypto current signature is not passed through the top-level metals, MIM capacitors, or on-board inductors, which are the main sources of EM leakage, thereby preventing EM SCA attacks.

References

[1] Paul Kocher et al. Differential Power Analysis. In *CRYPTO*, 1999.
[2] Colin O'Flynn. A Framework for Embedded Hardware Security Analysis. July 2017.
[3] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer US, 2007.
[4] Eric Brier et al. Correlation Power Analysis with a Leakage Model. In *CHES 2004*, pages 16–29, 2004.
[5] D. Das et al. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In *IEEE HOST*, 2017.
[6] Fox-IT. TEMPEST attacks against AES. Technical report.
[7] Naofumi Homma et al. EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor. In *CHES*, 2014.
[8] Daniel Genkin et al. Stealing Keys from PCs Using a Radio. In *CHES*, pages 207–228, September 2015.
[9] Daniel Genkin et al. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs. Technical Report 129, 2016.
[10] Josef Danial et al. SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing. *arXiv:1908.09407*, September 2019.
[11] Thomas Eisenbarth et al. On the Power of Power Analysis in the Real World. In *CRYPTO*, pages 203–220, 2008.
[12] Josep Balasch et al. Power Analysis of Atmel CryptoMemory – Recovering Keys from Secure EEPROMs. In *CT-RSA*, 2012.
[13] Amir Moradi et al. On the vulnerability of FPGA bitstream encryption against power analysis attacks. CCS, pages 111–124, 2011.
[14] J. Longo et al. SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip. In *CHES*, 2015.
[15] Debayan Das et al. Enabling Covert Body Area Network using Electro-Quasistatic Human Body Communication. *Scientific Reports*, 9(1), 2019.
[16] Shovan Maity et al. A 415 nW Physically and Mathematically Secure Electro-Quasistatic HBC Node in 65nm CMOS for Authentication and Medical Applications. In *CICC*, 2020.
[17] Giovanni Camurati et al. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. CCS, Toronto, Canada, 2018.
[18] Haider Adnan Khan et al. IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems. *IEEE TDSC*, 2019.
[19] Gabriel Hospodar et al. Machine learning in side-channel analysis: a first study. *Journal of Cryptographic Engineering*, 2011.
[20] Eleonora Cagli et al. Convolutional Neural Networks with Data Augmentation against Jitter-Based Countermeasures – Profiling Attacks without Pre-Processing –. Technical Report 740, 2017.
[21] Debayan Das et al. X-DeepSCA: Cross-Device Deep Learning Side Channel Attack. In *DAC*, 2019.
[22] Anupam Golder et al. Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. *IEEE TVLSI*, 2019.
[23] Debayan Das et al. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *HOST*, 2019.
[24] C. Tokunaga et al. Secure AES engine with a local switched-capacitor current equalizer. In *IEEE ISSCC*, 2009.
[25] M. Kar et al. 8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator. In *IEEE ISSCC*, 2017.
[26] A. Singh et al. A 128b AES Engine with Higher Resistance to Power and Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low-Dropout Regulator. In *ISSCC*, 2019.
[27] D. Das et al. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE TCAS I*, 2018.
[28] D. Das et al. 27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation. In *IEEE ISSCC*, 2020.
[29] D. Das et al. Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS. In *IEEE CICC*, 2020.