Ground-up Root-cause Analysis guided Low-Overhead Generic Countermeasure for Electro-Magnetic Side-Channel Attack

Debayan Das[1], Mayukh Nath[1], Baibhab Chatterjee[1], Santosh Ghosh[2] and Shreyas Sen[1]

[1] Purdue University, USA, {das60,nathm,bchatte,shreyas}@purdue.edu
[2] Intel Corporation, Hillsboro, OR, santosh.ghosh@intel.com

Abstract. The threat of side-channels is becoming increasingly prominent for resource-constrained internet-connected devices. While numerous power side-channel countermeasures have been proposed, a promising approach to protect the non-invasive electromagnetic side-channel attacks has been relatively scarce. Today's availability of high-resolution electromagnetic (EM) probes mandates the need for a low-overhead solution to protect EM side-channel analysis (SCA) attacks. This work, for the first time, performs a white-box analysis to root-cause the origin of the EM leakage from an integrated circuit. System-level EM simulations with Intel 32 nm CMOS technology interconnect stack reveals that the EM leakage from metals above layer 8 can be detected by an external non-invasive attacker with the commercially available EM probes. This work proposes a two-stage solution to eliminate the critical signal radiation from the higher-level metal layers. Firstly, we propose routing the entire cryptographic core using the local lower-level metal layers, whose leakage cannot be picked up by an external attacker. Then, the entire crypto IP is embedded within a signature attenuation hardware (SAH) which in turn suppresses the critical encryption signature and finally connects to the highly radiating top-level metal layers. We utilize the Attenuated Signature Noise Injection (ASNI) circuit, which was recently proposed as a low-overhead generic power SCA countermeasure, in order to encapsulate the cryptographic core with local low-level metal routing, and thereby significantly suppress the critical signatures even before it reaches to the higher metals. System-level implementation of the ASNI circuit with local lower-level metal layers in TSMC 65 nm CMOS technology, with an AES-128 core (as an example cryptographic engine) operating at 40 MHz, shows that the system remains secure against EM SCA attack even after $1M$ encryptions, with 67% power efficiency compared to the unprotected AES.

Keywords: EM Side-channel attack · Generic countermeasure · Ground-up EM Leakage Modeling · Cryptographic hardware · Attenuated Signature Noise Injection

1 Introduction

The huge growth of internet-connected devices has led to the development of strong and mathematically-secure cryptographic algorithms. Almost all embedded devices including mobile phones and smart cards employ encryption engines. However, unfortunately these algorithms are implemented on a physical platform, and these physical CMOS-based devices leak information in the form of power consumption [KJJ99], [BCO04], electromagnetic (EM) emanations [GMO01], [QS01], acoustic vibrations [GST14] or the timing of encryption operations [BB03]. These side-channel leakage information can be exploited by attackers to extract the secret key from an encryption device.

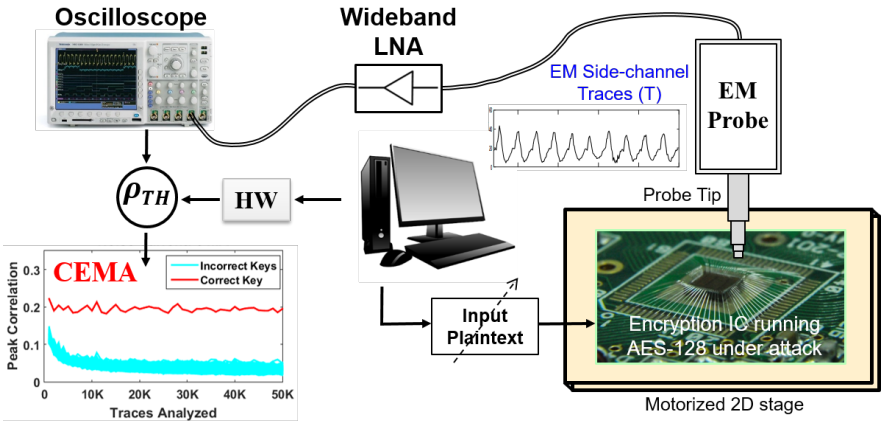

Figure 1: EM Side-Channel attack Overview

1.1 Preliminaries

The EM analysis attack is a prominent non-invasive side-channel attack (SCA) on cryptographic ICs and has been demonstrated over the last decade [GPPT15], [GPPT16]. EM side-channels provide a multi-dimensional spatial information over time [GMO01] and allows to separate the contributions due to different components of the ASIC, in contrast to the power analysis attacks, which can be visualized as information in a single dimension [QS01]. The EM analysis attack is typically performed in two stages. In the first phase, the attacker collects the EM emanations using an EM probe (electric/magnetic) optionally connected to a low-noise amplifier (LNA) placed in the vicinity of the encryption device under attack. In the second phase, the collected EM traces are subjected to simple (SEMA) or differential EM analysis (DEMA) [MBO+05] to extract the secret key of the encryption device.

Figure 1 shows how a EM side-channel attack is performed. Initially, the EM emanations of the device performing encryption is measured in an oscilloscope or a high-resolution analog-to-digital converter (ADC), and the EM traces (T) are collected over varying input plain-texts for the same secret key. Next, for a correlational EM analysis (CEMA) [LCC+06], a hypothetical EM leakage model like the Hamming weight matrix (H) is built which contains the expected EM leakage of the device performing a particular operation during encryption (like the S-box operation in the first round of AES), over the given plain-texts with all possible key bytes. This reduces the key search space of the AES-128 to 2^8=256 possibilities for each byte of the secret key. Finally the correlation co-efficient (ρ_{TH}) between the EM hypothesis (H) and the obtained traces (T) is calculated over time. One significant advantage of CEMA (or, CPA for correlational power analysis) is that the precise knowledge of the time instance when the targeted operation occurs is not required, since ρ_{TH} can be calculated at each sampling point of the trace. The key byte showing the maximum correlation represents the correct key byte. Repeating the process 16 times reveals the entire 128 bits of the secret key.

Even a low-cost software-defined radio USB stick or a consumer-grade radio receiver [GPPT15], as shown in Figure 2 can be utilized to capture the EM radiations from a distance and send the digitized data to a far-away (few metres) computing device wirelessly in real-time to perform CEMA/DEMA and thereby recover the secret key.

Real-world examples of EM SCA include the counterfeiting of e-cigarette batteries by stealing the secret encryption keys from the authentic batteries to gain market share. In general, electromagnetic analysis attacks can be used to extract the hidden key from the boot-loader of any embedded VLSI device [O'F17], [GPPT15], [GPPT16].

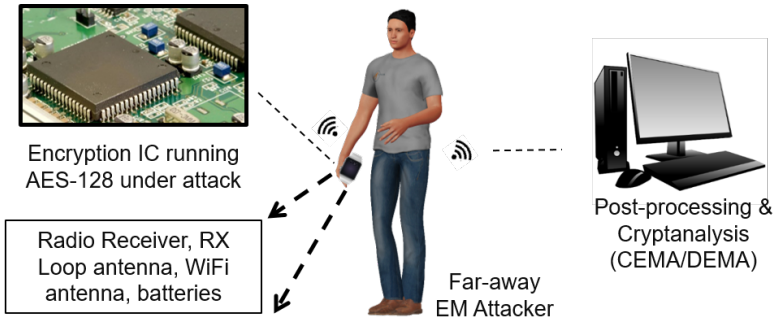

Figure 2: Non-invasive EM Side-channel attack from a distance: Attacker collects the EM traces of the encryption device using a portable USB-based radio receiver and transmits it wirelessly to a computer few metres away to perform CEMA/DEMA attacks to break the secret key.

1.2 Motivation

The ever-increasing demand for protected audio/video streaming, social media, and financial data transactions, has rendered high performance encryption a standard requirement for the majority of electronic systems. One of the most commonly used cryptographic algorithms present in most servers and mobile platforms is the Advanced Encryption Standard (AES). In order to support energy-constrained small form-factor IoT edge and hub devices, hardware accelerators for encryption algorithms are being actively studied. As edge/hub computing thrives to become more ubiquitous, ensuring security of these encryption engines with high energy-efficiency becomes increasingly challenging and critical. Consequently, power and EM side-channel attack on encryption ICs have gained tremendous importance over the last decade [MOP07], [GM11], [O'F17], [PSQ07]. Although researchers have mainly focused on countermeasures against power SCA, preventing EM attacks is gaining more prominence in the present era of IoT, due to the availability of commercial inexpensive EM probes. Being in the close proximity of the encryption device, the EM side-channel leakage can be captured non-invasively using low-cost EM probes, in contrast to the requirement for physical probing in power analysis attacks. Hence, a low-overhead generic countermeasure that can be commonly utilized for both power and EM side-channel resilience is extremely necessary.

This work performs a ground-up analysis to root-cause the origin of the EM leakage in an integrated circuit (IC). After identifying the source of the EM leakage, we investigate the existing state-of-the-art power and EM SCA countermeasures that can be utilized for protecting the cryptographic IC. Among the existing countermeasures, the recently proposed Attenuated Signature Noise Injection (ASNI) [DMN+18] is a generic and low-overhead solution to protect against power SCA. In this work, we utilize ASNI to embed the entire cryptographic IP of an electronic system with local low-level metal routing to significantly attenuate the signature before it reaches the top metal layers of the chip, which leaks critical information through EM side-channels.

In this article, as an application of the proposed countermeasure, we focus on a 128-bit AES engine. Correlation power/EM analysis (CPA/CEMA) with Hamming weight model [LCC+06] is employed for the attack.

1.3 Contribution

Specific contributions of this paper are:

- This work, for the first time, performs a ground-up root-cause analysis to develop the

fundamental understanding, i.e. a 'white-box model' of the source of EM information leakage from the current path from a cryptographic IC. System-level simulations using Ansoft HFSS for 32 nm Intel CMOS technology reveals that EM leakage is detectable using commercial probes from metal layers higher than 8.

- To eliminate the critical signature radiation from the higher-level metal layers, a two-stage solution is proposed. (1) Electric field Suppression: The cryptographic IP is routed through the local lower-level metal layers, reducing EM leakage. However, due to high routing resistance, low-level routing could only be local and cannot be routed to the metal pads of the chip. This calls for the (2) Signature Suppression: The encryption signature needs to be highly suppressed before it is routed to the global higher metal layers. A combined effect of local E-field Suppression and the Global Signature Suppression is the key to minimizing EM side-channel leakage.

- In order to suppress the AES encryption (or the whole crypto IP) signature, this work utilizes Attenuated Signature Noise Injection (ASNI) technique, that attenuates the correlated AES current signature significantly before it reaches the higher metal layers.

- CEMA attacks implemented on ASNI-AES show that none of the secret key blocks have been disclosed even with $1M$ traces (Minimum Traces to Disclosure (MTD) $> 1M$), with only $1.23\times$ area overhead, $1.5\times$ power overhead compared to the unprotected AES, without any performance penalty.

1.4 Paper Organization

The remainder of the paper is organized as follows. Section 2 provides the background and summarizes the existing countermeasures against EM SCA. In Section 3, the ground-up EM modeling of the interconnect stack for the Intel 32 nm CMOS process is presented. Section 4 discusses the simulation results of the EM leakage analysis from the metal layers. In Section 5, we propose a low-level metal layer hardware countermeasure (ASNI) to shield the cryptographic IP signature variations from reaching the top metal layers. Section 6 discusses the implementation results of the ASNI-AES and its efficacy against EM SCA attacks. Section 7 concludes the paper.

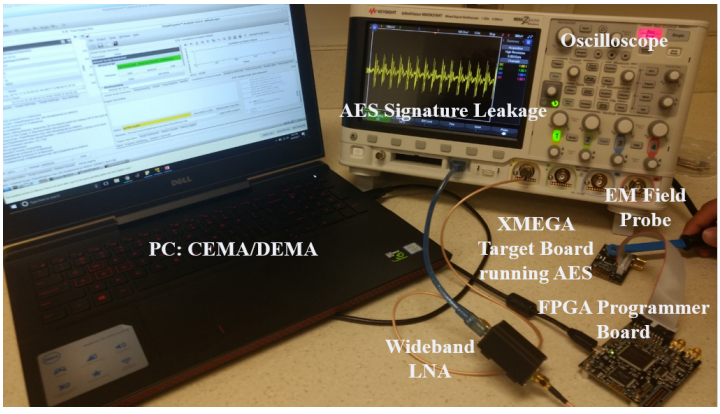

Figure 3: EM Side-Channel attack Laboratory Measurement Set-up

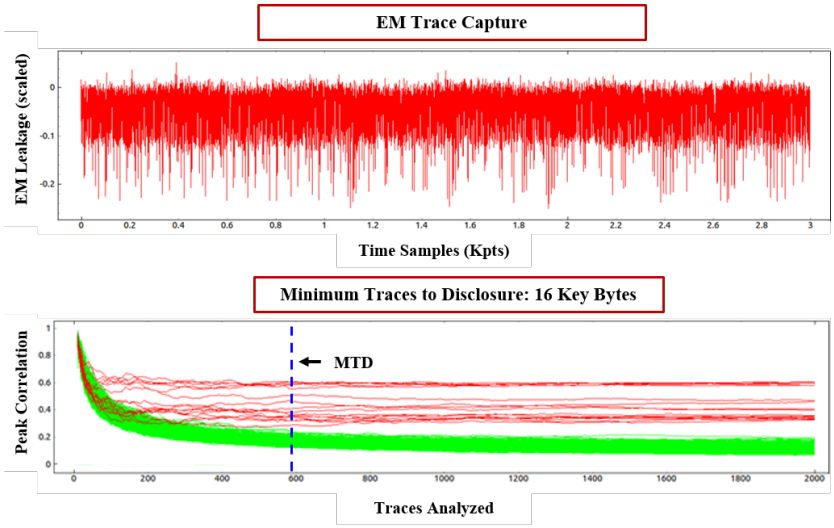

Figure 4: Correlation EM Side-channel attack on the Atmega microcontroller running AES-128. (a) The EM traces gathered from the oscilloscope, (b) CEMA attack on the unprotected AES core shows $MTD < 600$ traces.

2 Background & Related Work

Figure 3 shows a laboratory set-up involving a target Atmega microcontroller board (Chipwhisperer Lite board) [OZ14] running AES-128 encryption and the EM field picked up by a nearby EM probe connected to a low-noise amplifier (LNA) and is captured using an oscilloscope. The oscilloscope data is then downloaded to a laptop/PC wherein the correlation EM analysis (CEMA) is performed to reveal each byte of the secret key. As seen from Figure 4, all the 16 key bytes of the AES-128 implementation can be obtained within < 600 traces, thereby breaking the security of this system. Although this is a basic example to prove the feasibility of EM SCA, it demonstrates the potency of EM SCA attacks on electronic systems.

2.1 Literature Review: Black Box Approach

Several EM side-channel attacks have been demonstrated over the last few years. In CHES 2002 [AARR02], it was first shown that the EM spectrum could be sensed to perform SCA. There have been few works to scan the EM emissions of integrated circuits in time-domain [OLS+08]. Lomne et al. [LMT+09] proposed a modeling of magnetic emissions from ICs using Redhawk. Recently, Kumar et al. [KSYO17] proposed an efficient simulation set-up to perform EM SCA. However, most of these works focus on top-down modeling of EM emissions from a chip and consider the cryptographic IC as a black box. In CHES 2014 [HHM+14], the authors developed an on-chip sensor to detect an approaching probe. Another demonstration of EM SCA using cheap off-the-shelf components was shown in CHES 2015 [LMPT15]. In addition, the development of highly sensitive EM probes [GPPT15] calls for a fundamental understanding of the characteristics of EM side-channel leakage from cryptographic ICs and trace the critical information-leakage sources in the current path.

Specific countermeasures proposed against EM SCA include signal strength reduction techniques like shielding or signal information reduction using noise insertion [AARR02]. However, data randomization with noise injection comes with significant power overheads, and EM shielding incurs high cost of packaging [YTK+10]. To the best of the authors'

knowledge, none of these works have throughly investigated the critical sources of the EM leakage in a cryptographic IC. Hence, in this work, we perform a bottom-up analysis of the components within an IC that causes the EM emanations, and propose low-overhead energy-efficient countermeasures against EM SCA. In addition, our goal is to protect both power as well as EM SCA with a single effective and generic countermeasure.

2.2 Genesis of the EM Leakage: A White box Approach

Although the source of leakage in the case of power analysis attack is well understood and analyzed [MOP07], [RBN+15], [DMN+17], the origin of EM leakage in the context of side-channel security is still not well-perceived. In this work, we conceive a ground-up approach to analyze and root-cause the genesis of this EM side-channel leakage in a CMOS IC.

In any problem on electro-magnetics, the sources of excitation can be broken down into two basic elements, namely charge density ρ and current density $\vec{J}$. The presence or absence of ρ and J, and their static or time-varying nature determines the electric field, magnetic field, and electromagnetic radiation present in the system. These outcomes can conveniently be derived from the four Maxwell's equations. The differential forms of the Maxwell's equations are shown in Eqns. 1 - 4 [Gri17], where $\vec{E}$ is the electric field in V/m, $\vec{H}$ denotes the magnetic field intensity in A/m, $\vec{J}$ is the electric current density in A/m^2, ρ denotes the electric charge density in C/m^3, ϵ is the electric permittivity and μ is the magnetic permeability of the medium.

$$\nabla \cdot \vec{E} = \frac{\rho}{\epsilon} \tag{1}$$

$$\nabla \cdot \vec{H} = 0 \tag{2}$$

$$\nabla \times \vec{H} = \vec{J} + \epsilon \frac{\partial \vec{E}}{\partial t} \tag{3}$$

$$\nabla \times \vec{E} = -\mu \frac{\partial \vec{H}}{\partial t} \tag{4}$$

In an integrated CMOS-based circuit, in steady-state, there is no static current flowing through the circuit. However, the presence of stationary charges in the circuit give rise to electric fields ($\vec{E}$), as can be explained from Gauss' Law (Eqn. 1). As the output of logic gates switches its state, moving charges (dynamic and leakage currents) create changing electric fields, which in turn produce magnetic fields (known as modified Ampere's law - Eqn. 3). On the other hand, changing currents (acceleration of charges) produce time-changing magnetic flux, thereby inducing an electric field, which is known as the Faraday's law (Eqn. 4).

The present day CMOS architecture consists of a cell-level transistor layer over a silicon substrate, and multiple layers of metal consisting of interconnects and vias [NAB+08]. Depending on different CMOS technologies, the number of total metal layers may vary. However, having more number of metal layers is important for integrated circuit designs as it not only makes it easier for the circuit designer, but also reduces the area of the chip significantly as the layers are stacked on top of another. The highest metal layers available for a process are used as the power grid. Hence, any signal in the lower-level metal layers have to be routed to the topmost metal layer and through to the copper (Cu) bump, as shown in Figure 5(b).

As a result, any cell-level excitation is reflected as a time-varying current through the metal layer routings. The interconnects in the routing, due to the presence of this time-varying current, start functioning as antennas, and emits electromagnetic radiation.

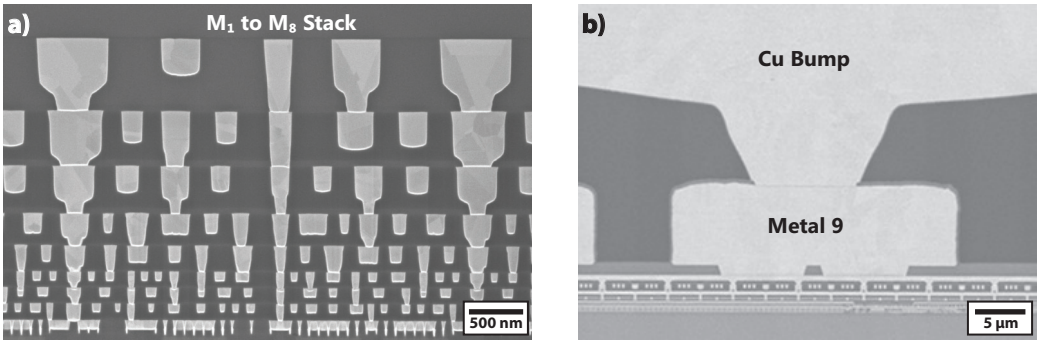

Figure 5: Cross-Section of the Interconnect Stack (Intel 32 nm) [NAB+08], (a) Metal 1 through 8 (b) Includes metal 9 and the copper bump layer.

Now, the typical operating frequency (f) of industrial digital CMOS circuits lie in the 1-10 GHz range, which corresponds to a wavelength $\lambda = \frac{v}{f}$ (v denotes the speed of propagation of the EM waves and $v = 3 * 10^8 m/sec$), which is in the order of 30-300 mm, whereas the dimensions of the interconnects are usually three orders of magnitude lower, in the range of few micrometers. This type of excitation structure, where the length of the interconnects $l \ll \lambda$, is analogous to infinitesimal dipoles in antenna theory [Bal16]. For an infinitesimal dipole, the excitation frequency lies far away from the resonant frequency of the antenna, and hence the structure can be analyzed assuming a uniform current amplitude I_0 throughout its length. This is unlike a traditional half wavelength ($\lambda/2$) dipole antenna, where the excitation frequency matches the antenna resonance, and the current distribution forms nodes and anti-nodes along the length of the antenna. Now, as the current distribution in an infinitesimal dipole is uniform, it can be intuitively broken down into unit elements, wherein each element contributes equally (E_i) towards the net radiated field amplitude E_{rad}. If N is the number of elements, $E_{rad} = NE_i$, and as a matter of fact, N is proportional to the dimensions of the radiation structure. As a result, the radiated field amplitude should have a linear dependence on the dimensions of the structure, e.g. if the length of the structure is l, $N \propto l$ and $E_{rad} \propto N$, so $E_{rad} \propto l$. The radiated power P_{rad} would then be proportional to l^2. In fact, for infinitesimal dipoles, the radiated power can shown to be proportional to $(l/\lambda)^2$, as given by Eqn. 5, [Bal16]

$$P_{rad} = \eta \left(\frac{\pi}{3}\right) \left|\frac{I_0 l}{\lambda}\right|^2 \tag{5}$$

where $\eta = \sqrt{\mu/\epsilon}$.

Thus in essence, the time-varying electric and magnetic fields produce an EM wave during the switching activity of the logic and sequential circuits within an ASIC. A nearby attacker can pick up the radiated "side-channel" EM emissions and extract the secret key from the encryption engine using CEMA/DEMA. It is therefore essential to understand the origin and exact nature of the radiation from the metal layers in a chip to devise a design strategy in order to counter EM SCA. Also, the magnitude of the EM fields depends on the amount of current flowing in the circuit and the dimensions of the metal layer routings. Following this general idea, we design the model of interconnect stacks to study the effect of metal layer dimensions to the EM radiation signature.

Table 1: Pitch and thickness of metal layers at Intel's 32 nm node [NAB+08]

Layer	Pitch(nm)	Thickness(nm)
Metal 1	112.5	95
Metal 2	112.5	95
Metal 3	112.5	95
Metal 4	168.8	151
Metal 5	225.0	204
Metal 6	337.6	303
Metal 7	450.1	388
Metal 8	566.5	504
Metal 9	19.4 µm	8 µm
Bump	145.9 µm	25.5 µm

3 Modeling EM Emanation from Metal Layers in Modern CMOS Process: Interconnect Stack

As discussed in the previous section, the EM radiation from a CMOS IC primarily originates from the metal layer routings. To develop a better understanding of the situation, the net radiation can be split into contributions originating from each individual interconnect in the routing. A simple structure that can be used to analyze the radiation properties of different metal layers is a vertical stack of interconnects, joined by vias. We have chosen the dimensions of the interconnects in different layers in accordance with Intel's 32 nm technology node as listed in Table 1 [PAA+09]. The cross section of the targeted structure

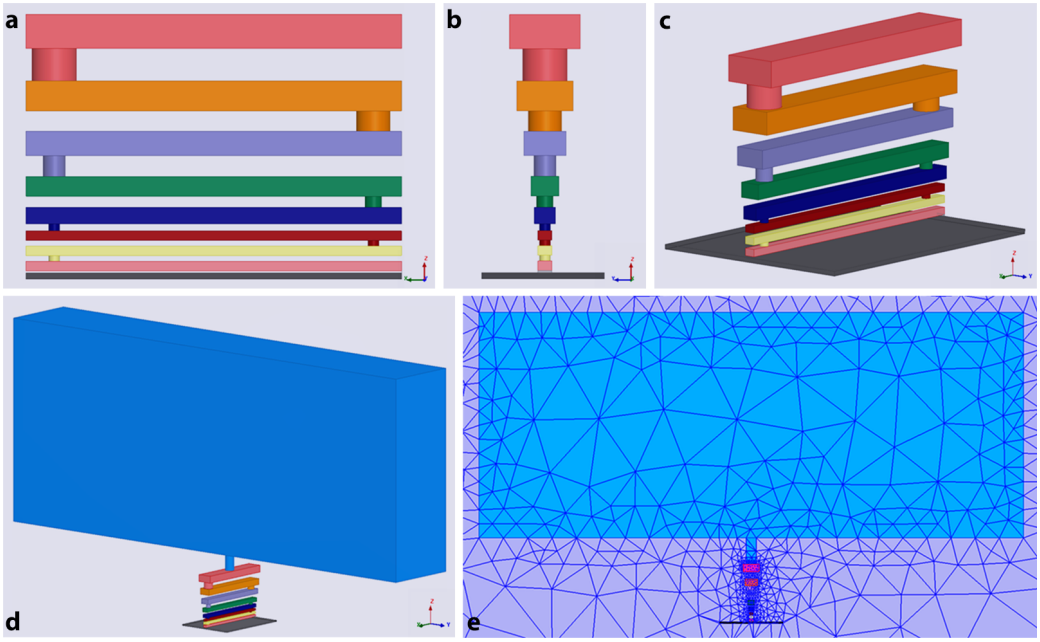

Figure 6: Modeling the Interconnect Stack for the Intel 32 nm CMOS process: (a) Metal 1-8 side view, (b) cross-sectional view, and (c) isometric projection; (d) isometric projection with metal layer 9 included; (e) adaptive meshing in HFSS.

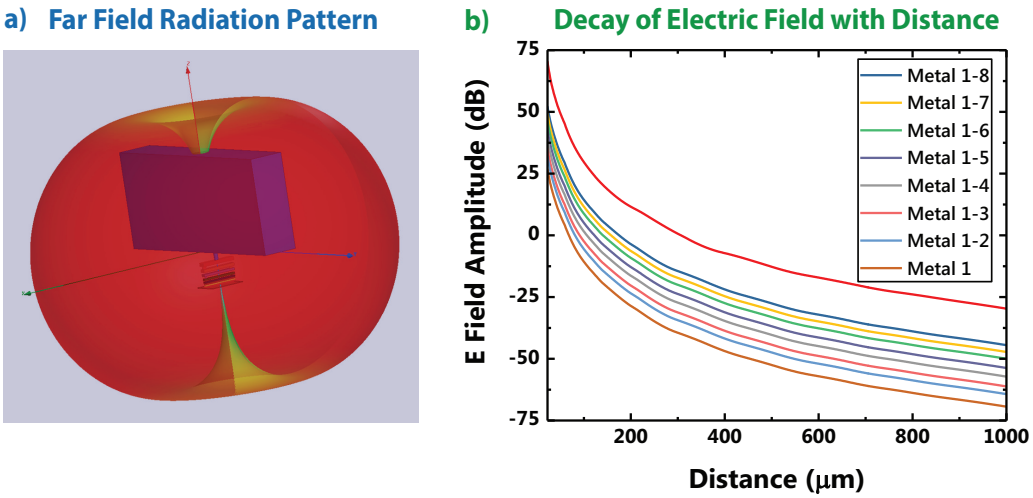

Figure 7: Simulation Results at 1 GHz excitation: Field Pattern. (a) Far-field radiation pattern, (b) E-field decay of the metal layers with distance.

is shown in Figure 5 and the resulting model is shown in Figure 6. We use Ansoft HFSS, a finite element method (FEM) based EM simulator to solve Maxwell's equation in the system. The excitation to the system is provided via a lumped port in HFSS between the bottom-most metal layer and a perfect electric conductor (PEC) plate functioning as a ground. This style of excitation is similar to the feed of a dipole antenna, and is justified due to the similarity of the system to an infinitesimal dipole, as described in the preceding section. The length of each interconnect layer is taken to be 3 µm. A sphere of radius 1 mm enclosing the interconnect stack is used as the simulation region to limit the simulation to a finite volume. Radiation boundary is applied at the surface of the spherical region to eliminate reflection of incident radiation from the outer surface of the simulation region.

Contribution of different Metal Layers

This interconnect stack system is solved at 1 GHz and the electric field amplitude is documented as a function of distance from the structure. The far-field radiation pattern, as shown in Figure 7(a), is analogous to that of a dipole antenna [Bal16], as postulated. We repeat the simulation multiple times, eliminating the topmost metal layer in each subsequent run, and plot the decay of radiated electric field with distance for each structure, as shown in Figure 7(b). This allows us to estimate the radiation contribution of each individual metal layer. e.g. the difference between the E-field amplitudes obtained for M_{1-9} and M_{1-8} provides a first order estimate for the radiation emanated by metal layer 9.

4 EM Leakage detection from the metal layers: Simulation Results

To quantify the contribution of each layer at a particular distance from the probe (D), we use the simulated field amplitudes at $D = 900\mu m$ (Figure 8) and compute the difference between adjacent traces. The individual contribution of the layers to the field show a strong linear correlation with the dimensions of the metal layers. This is shown in Figure 8(d)

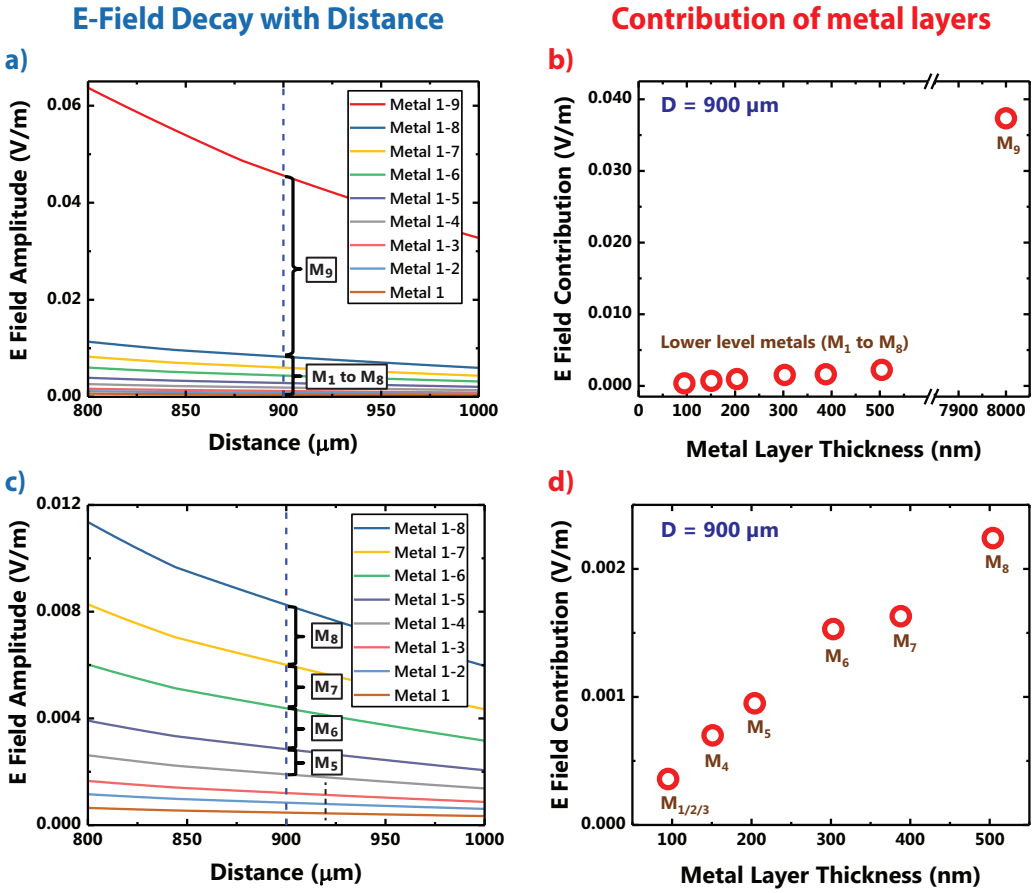

Figure 8: (a) E-field amplitude for the metal stack (layers 1 through 9) reduces as each layer is eliminated, (b) Contribution of Metal Layers 1 to 9, (c, d) E-field contributions of the metals 1 through 8, showing a linear relation with the dimension of the metal layers.

where E field contributions of M_1-M_8 is plotted against the thickness of those layers. The thickness of M_9 increase by a factor of 16 from M_8, and this is translated into the radiation contribution from M_9 as well, as seen in Figure 8 (a) and (b).

Hence, Figure 8 shows that the radiation from top-level metal layers in a CMOS IC is significantly higher compared to that from the lower levels. It is therefore imperative for an EM SCA countermeasure strategy to minimize the radiation from top-level metal layers, for excitations that originate from the cell level. In fact in this specific example of excitation model using the Intel 32 nm interconnect stack dimensions, if the radiation contribution from M_9 is eliminated, the net radiation at 900 µm drops below the sensitivity of commercially available E-field probes.

Accordingly, the detectable EM leakage from the metal layers can be formulated in terms of the noise floor ($NF_{oscilloscope}$) of the oscilloscope, the transfer function of the electric field (E) to current (I) for different metal layers (M_X) and the response of the E-field probe (Figure 9), as shown in Eqn. 6.

$$i_{AES}(E_I)_{M_X}(V_E)_{probe} \geq NF_{oscilloscope} \tag{6}$$

The total electric field measured by the external probe is the sum of contribution from

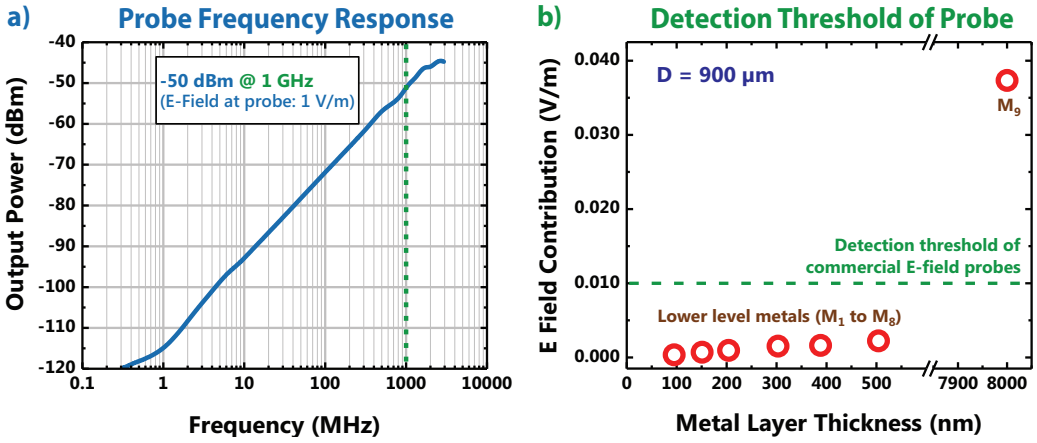

Figure 9: Sensitivity of the commercial E-field Probes: (a) Frequency Response of a commercial E-Field probe [Sol], (b) At $D = 900\mu m$, a commercial E-field probe can potentially detect radiation from Metal Layer 9 (Intel 32 nm process).

the AES engine ($E_{I_{local}}$) and the unrelated logic ($E_{I_{global}}$) present in the circuit, as given in Eqn. 7. $E_{I_{global}}$ is the electric field from the global chip routing, whereas $E_{I_{local}}$ is from the local routing of the AES engine. Hence, typically, the AES engine is a small portion of the whole chip, that is, $E_{I_{global}} \gg E_{I_{local}}$.

$$E_I = E_{I_{local}} + E_{I_{global}} \tag{7}$$

The electric field E_I is measurable as long as the output voltage from the E-field probe (depending on the V_E transfer function of the probe) is above the noise floor of the oscilloscope (measured to be $\approx -90dBm$ ($20\mu V_{pp}$) at a frequency of 1 GHz). Hence, as seen from Figure 9, the detectable E-field is $\sim 10mV/metre$, which means that EM leakage from the metals (for length $= 3\mu m$) up to the layer 8 in Intel 32 nm technology is not detectable. However, depending on the technology process, different metal layers may radiate above the detectable threshold giving rise to EM SCA vulnerability.

5 Low Overhead Generic Countermeasure against EM SCA

In the previous section, it has been shown that the the source of measurable EM leakage are the topmost metal layers in a cryptographic IC. This is a very critical observation which is the crucial aspect in developing a low-overhead countermeasure against EM SCA. Hence, our goal is to protect those metal layers from leaking sensitive information during the AES encryption.

In this regard, if we can somehow completely shield the top metal layer (M_9 for our example with Intel 32nm process) by suppressing the encryption signature even before it reaches M_9, then there would be no EM leakage from the encryption IC. Thus, solving the EM SCA problem is reduced to solving the power SCA problem in the lower-level metal layers, that is, suppressing the AES signature completely before it reaches the top-level metal layers. Keeping this in mind, we can utilize the power SCA countermeasures that can strongly suppress the AES signature.

Power SCA countermeasures include power balancing, hardware masking, noise injection, and supply isolation. Power balancing logic implementations include sense-amplifier based logic (SABL) [TAV02], dual-rail circuits [BGLT06], and wave dynamic differential logic (WDDL) [HTH+06]. WDDL is the first power attack resistant power-balancing circuit

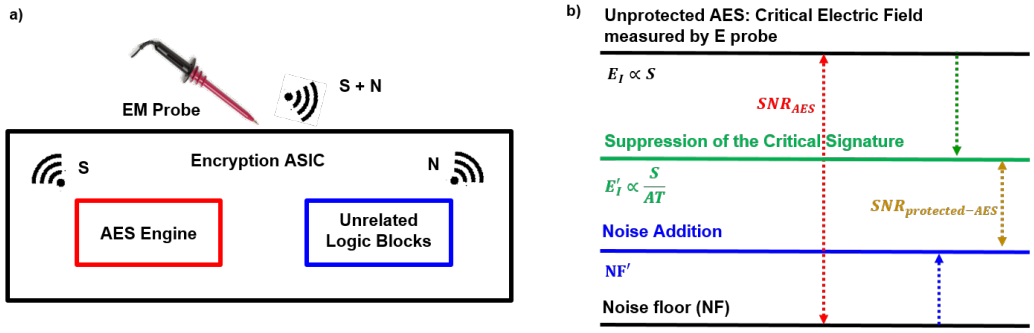

Figure 10: (a) Critical Signal Leakage (S) and the noise (N) due to other components in an integrated circuit; (b) the Signal-to-Noise ratio can be reduced by either noise addition or by suppressing the critical encryption signature.

validation on silicon, with a MTD of $21K$. However, the enhanced protection consumed 3× area overhead, 4× power and a 4× performance degradation.

Hardware masking is a logic-level countermeasure that involves replacing each logic gate with a sophisticated one to obfuscate the power consumption and achieve gate-level masking, leading to high power and area overheads (> 4×) [RBN+15], [CEM18]. Another recent AES-128 architecture-specific countermeasure [YK17] proposed using a fixed intermediate mask (false-key masking) and combined with WDDL-based XOR gates for reconstruction of the original cipher claims a low-overhead solution. However, the solution only works for a fixed-key based AES implementation as dynamic keys would need a random mask, which would significantly increase the power and area overheads (> 2×).

Physical countermeasures include noise injection, switched capacitors, integrated voltage regulators (IVRs), and attenuated signature noise injection (ASNI). Noise injection alone

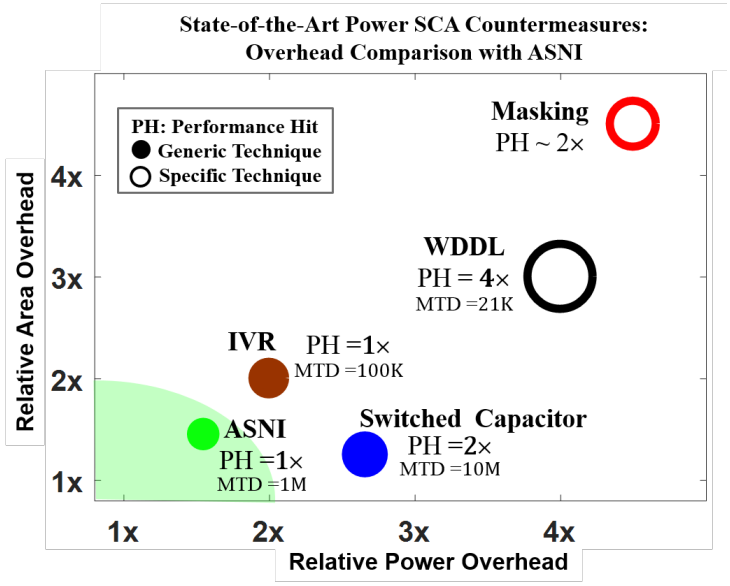

Figure 11: Overhead comparison of the existing State-of-the-art hardware SCA countermeasures with ASNI [DMN+18]. MTD refers to the Minimum Traces to Disclosure. Performance hit (PH) = 1× implies no performance degradation.

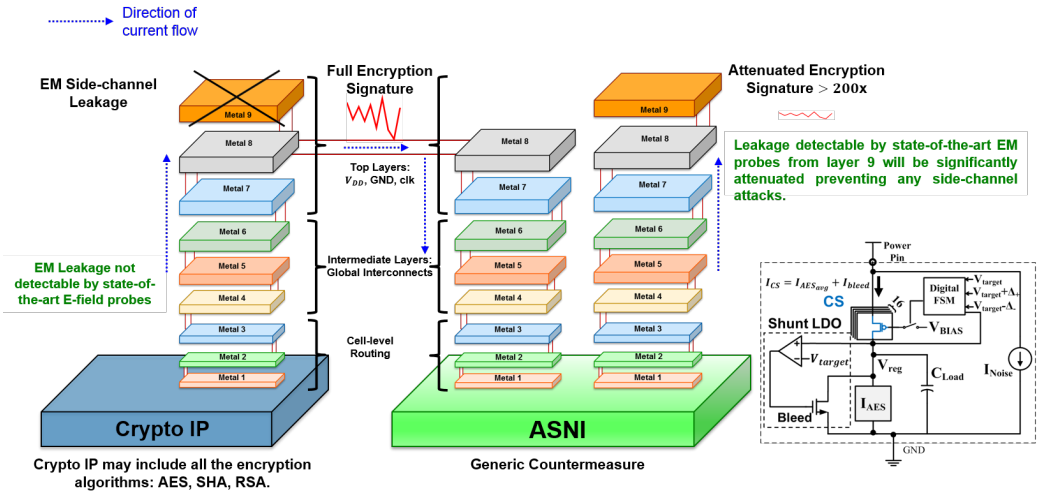

Figure 12: EM Side-Channel Attack Protection using ASNI

incurs very high power overheads ($> 15\times$ to achieve MTD of $50K$) [GM11], [DMN+17] and is not an optimum solution. The switched capacitor current equalizer module proposed by Tokunaga et al. [TB10] is a novel technique against power SCA, however it resulted in a $2\times$ performance degradation in addition to the 33% power overhead. IVR-based implementations utilize traditional low-dropout regulators (LDOs) [SKR+16] and buck converters [KSM+17]. However, an ideal LDO-based implementation is inherently insecure as the supply current reflects the changes in the load (AES) current. Hence, the above LDO-based techniques introduce non-idealities in the system and thereby incur a fundamental trade-off between the system performance (like dynamic loop response) and side-channel resilience. On the other hand, buck-converter based IVRs require large passives and thus consume $> 2\times$ power and area overheads. IVRs use the wirebond inductances, which can leak critical information in the form of EM emanations. Hence, this IVR-based countermeasure cannot be directly used for protecting against EM SCA.

Recently, Attenuated Signature Noise Injection (ASNI) has been proposed as a low-overhead generic countermeasure against power SCA [DMN+18]. It embeds the AES engine in a Signature Attenuating Hardware (SAH) which highly suppresses the variations in the AES signature with significantly low overhead. As the AES signature gets attenuated by $> 200\times$, a very small noise injection can decorrelate the power traces such that the traces obtained by probing at the observable power pin are independent of the AES transitions ($MTD > 1M$). As shown in Figure 10, ASNI reduces the signal-to-noise ratio (SNR), both by strongly suppressing the signature, followed by tiny noise injection. Hence, as an EM SCA countermeasure, we utilize the ASNI circuit built locally on top of the crypto IP with lower-level metal layers so as to restrict the signature from reaching the topmost metal layers which radiates significantly. The overhead comparison of the related power SCA countermeasures is summarized in Figure 11.

Figure 12 shows the routing of the crypto IP through the local low-level metal layers 1 through 8, which is connected to the global higher metal layer 9 (whose leakage is detectable by commercially available probes) through the signature attenuation hardware in the form of ASNI. Hence, the AES-128 core is embedded within the ASNI which routes the attenuated signature through to the global higher metal layers and finally connected to the chip pads, as illustrated in Figure 13(a). The cross-sectional block-level view of the ASNI-AES (Figure 13(b)) shows the current flow through the metal layers connecting the AES-128 and the ASNI with the metal layers. The AES-128 core embedded within the

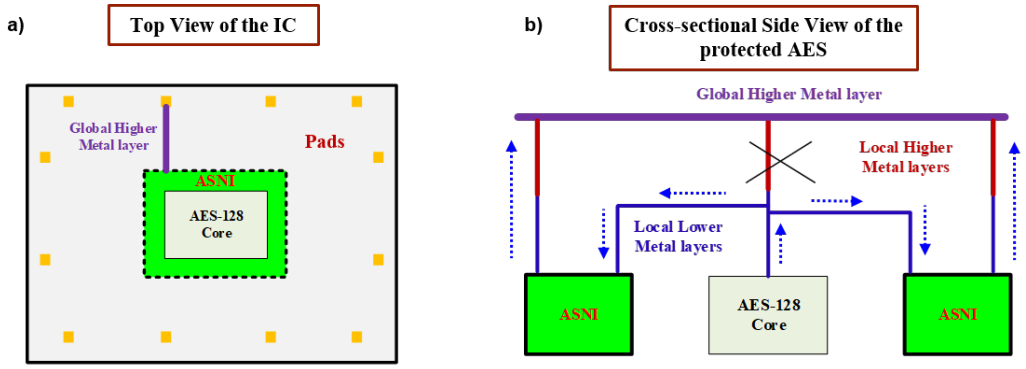

Figure 13: (a) Top level view of an integrated circuit with the AES-128 encryption engine embedded within the ASNI hardware; (b) A cross-sectional side-view of the ASNI-AES shows that the higher metal layers are isolated from the AES core, thus carrying a highly suppressed encryption signature after being passed through the ASNI circuit.

ASNI block is routed using the local lower metal layers, which connects directly to the global higher metal layers.

Figure 14(a) shows the traditional AES with parallel noise incorporation to obfuscate the supply traces [DMN+17]. I_{ov1}, I_{ov2} denotes the total overhead currents for the traditional AES with noise injection (NI) alone and ASNI-AES respectively. The underlying idea of ASNI is to embed the encryption engine (AES) in a signature attenuating hardware (Figure 14(b)), such that the variations in the AES current is highly suppressed and is not reflected in the supply current traces, thereby requiring significantly lower noise current injection to decorrelate the measured supply traces (Figure 14(c)).

5.1 Theory & Analysis of ASNI

ASNI uses a signature attenuation hardware (SAH) to attenuate (attenuation factor = AF) the AES signature so that the supply current (I_{CS}) becomes highly independent (high

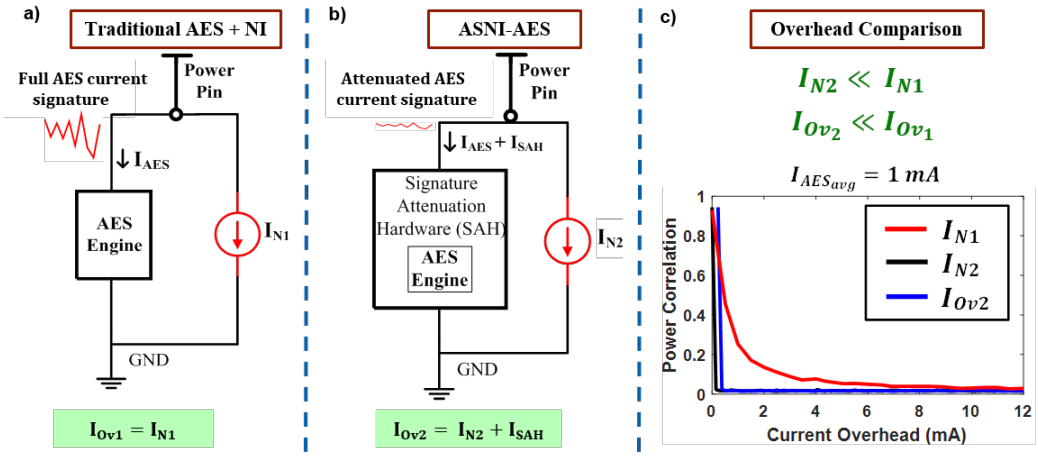

Figure 14: (a) Traditional AES with Noise Injection (NI), and (b) ASNI-AES, (c) Comparative Overview [DMN+18].

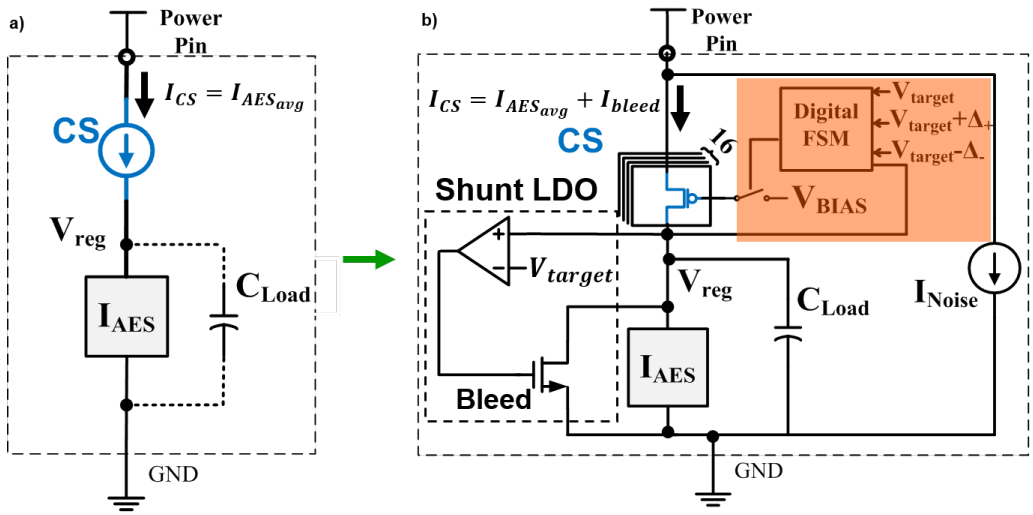

Figure 15: Build-up to the SAH: (a) An ideal implementation, (b) Proposed ASNI-AES architecture with noise injection to defend against power side-channel attacks [DMN+18].

attenuation: $AF \rightarrow 0$) of the AES signal transitions. The build-up to the SAH is shown in Figure 15. Figure 15(a) shows an ideal implementation involving an ideal constant current source on top of the AES engine, with an integrating load capacitor (C_{Load}) to account for the differences in the constant supply current and the variable AES current. This ideal topology only works if the constant current source supplies the average AES current $i_{AES_{avg}}$ over time. However, practically it is not feasible since if $I_{CS} > i_{AES_{avg}}$, the output voltage (V_{reg}) approaches V_{DD} (supply voltage) with time, due to the integration effects of the load capacitor, without any voltage regulation. Again, when $I_{CS} < i_{AES_{avg}}$, the output voltage (V_{reg}) approaches $0V$ with time, without any regulation. Hence, the constraint that the supply current needs to be set to the average AES current is not practical and leads to a meta-stable state of operation without ensuring proper regulation of the output voltage, leading to a performance hit.

Hence, as shown in Figure 15(b), a shunt low-dropout (LDO) regulator loop with a bleed device (NMOS) is used to dissipate the overhead residual current (I_{bleed}) and thus acts as a correction mechanism to compensate for the integration effects of the load capacitor, as shown in Figure 15. This topology called the shunt LDO-based control loop senses V_{reg} and controls the bleed NMOS gate voltage to draw the difference of current between I_{CS} and I_{AES}. Thus, this circuit is able to simultaneously regulate V_{reg} while keeping I_{CS} independent of I_{AES}, that is providing a time-variant significant attenuation by switching between small-signal and large-signal domains given by the Eqns. 8, 9 respectively [DMN+18], where $S = j\omega$ denotes the laplace variable.

$$AF_{SS} = \frac{i_{CS}}{i_{AES}} = \frac{g_{ds}}{C_{Load}} \left[\frac{S + a}{S^2 + S(p + \frac{g_{ds}}{C_{Load}}) + \frac{p(g_m A_v + g_{ds})}{C_{Load}}} \right] \tag{8}$$

$$AF_{LS} = \frac{i_{CS}}{i_{AES}} = \frac{g_{ds}}{g_{ds} + SC_{Load}} \tag{9}$$

Another switched-mode control (SMC) digital loop tracks the large changes in the average AES currents and compensates for any process, temperature or voltage variations. However, once the supply current is set, the SMC loop is disengaged (grayed out in Figure 15(b)) in the steady-state operation of the SAH.

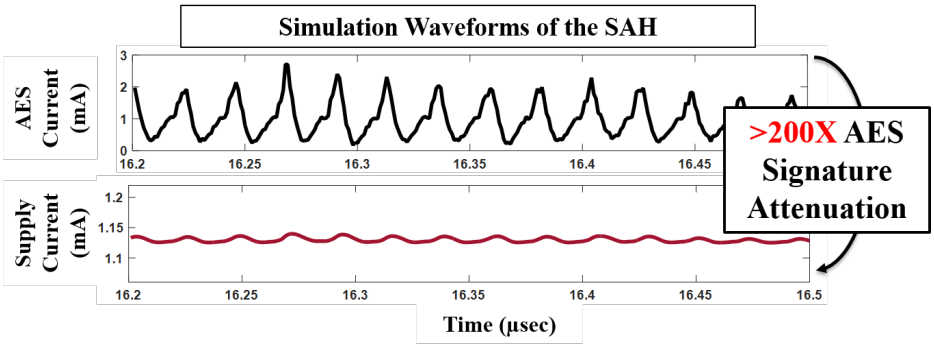

Figure 16: Snapshot of the time-domain waveforms of the SAH.

The SAH provides high attenuation (1/AF) and the attenuation factor (AF) depends on the choices of the load capacitor (C_{Load}), amount of overhead bleed current (i_{bleed}), the gain of the op-amp (A_v), transconductance of the bleed NMOS (g_m), placement of the dominant pole of the op-amp (p), and also the output resistance (r_{ds}, $g_{ds} = 1/r_{ds}$) of the current source (PMOS). Since an ideal current source is not feasible, a finite r_{ds} would reflect relative change in the output voltage (V_{reg}) in the supply current, however it will be highly attenuated ($> 200\times$), as seen from the time-domain waveforms of the ASNI-AES (Figure 16). Hence, a tiny amount of random noise current is injected (as shown in Figure 15(b)) to decorrelate the supply current traces with the estimated HW matrix, thereby providing significant immunity against CPA/CEMA attacks. The amount of noise injection required, as well as the total current overhead for ASNI is quantitatively analyzed in Section 6.1.

6 Local ASNI around Crypto-IP with low-level metal routing

In the previous section, we have investigated the power SCA countermeasures and chose ASNI as the suitable solution to provide significant attenuation to the AES signature with extremely low power/area overheads. In Section 4, we have also analyzed that the EM emanations from metal 9 is detectable using commercial EM probes for the Intel 32 nm CMOS process. Hence, if we "shield" the high-level metal layer (M_9 in this case) with the ASNI hardware (Figure 12, 13), then the AES signature cannot be detected by an external EM attacker. Hence, we propose development of a local ASNI that can be placed on top of the AES-128 core designed in 65 nm CMOS process.

The placement of the AES core encapsulated by the ASNI circuit (ASNI-AES) is very critical and has security, power and performance trade-offs. To achieve the highest security against EM SCA (maximum MTD), the ASNI-AES needs to be routed with the lowest metal layers. Although it provides minimum noise injection overhead, lower metal layers suffer from high resistance and may result in high voltage drop across the output voltage (V_{reg}), which can degrade performance (leading to lower throughput) of the AES encryption engine. AES-128 core designed in 130 nm CMOS technology consumes an area of $0.35mm^2$ [DMN+18]. Assuming that the maximum length of routing is $L_{max} = 350\mu m * \sqrt{2} = 493\mu m$ and we can tolerate an output voltage drop of $10mV$, the maximum tolerable resistance in routing is given by Eqn. 10.

$$R_{max} = \frac{\Delta V_{max}}{i_{AES_{avg}}} = \frac{10mV}{1mA} = 10\Omega. \tag{10}$$

$$R_{L_{max}} = \frac{R_{max}}{R_{L_{max}}} = \frac{10\Omega}{493\mu m} \approx 0.02\Omega/\mu m \tag{11}$$

Hence, we can route the ASNI-AES core only with metal layers for which $R < R_{L_{max}} = 0.02\Omega/\mu m$. Now, considering the Intel 32 nm CMOS process, as shown in Figure 5(b), only metals above layer 7 can provide the desired low routing resistances and hence provides no performance degradation of the operation of the cryptographic core. Hence, the AES can be routed up to metal layer 7 (as shown in Figure 12) and shielded with the ASNI hardware so that signals leaking to top-level metal layers are highly attenuated. However, the placement of the ASNI-AES core needs to be analyzed in design-time depending on the particular process (CMOS technology).

Using the local ASNI as an EM SCA countermeasure, it provides an attenuation ($\frac{1}{AF}$) to the AES signature such that the measured electric field (Eqns. 6, 7) gets modified accordingly as shown in Eqns. 12, 13, 14.

$$E_{I_{ASNI}} = \frac{E_{I_{local}}}{AT_{local}} + \frac{E_{I_{global}}}{AT_{global}} \tag{12}$$

$$AT_{local} = \frac{M_9}{M_{X_{Crypto}}} : \textit{E-field reduction due to absence of higher local metal layers} \tag{13}$$

$$AT_{global} = \frac{1}{AF_{ASNI}} : \textit{Crypto/AES Signature Suppression using ASNI} \tag{14}$$

Hence, as seen from Eqns. 13, 14, the overall SNR reduction has two key components: (1) Electric field suppression achieved due to the absence of routing through the local high-level metal layers. In this case, if the AES-128 core embedded within the ASNI block is routed with local low-level metal M_1 to M_7 (meeting the constraint presented in Eqn. 10, 11), then the ASNI hardware can directly connect to the global high-level metal M_9, and thus $AT_{local} = \frac{M_9}{M_7} \approx 20$ (from Table 1). (2) AES Signature suppression using ASNI, although the EM signal leakage from the global metal layers remain the same, but the correlated signature present in the emanated E-field is significantly attenuated.

Now, the ratio of the electric fields contributed by the local and global routing from the AES block can be attributed to the relative area of the AES to the area of the rest of the circuit, as given in Eqn. 15,

$$\begin{aligned} \frac{E_{I_{local}}}{E_{I_{global}}} &= \frac{\text{Area of the AES}}{\text{Area of the rest of the chip}} \\ &\approx \frac{200\mu \times 200\mu}{1m \times 1m} = \frac{1}{25}. \end{aligned} \tag{15}$$

Now, from Eqn. 7 and Figure 8(a), we see that for an excitation of 1V with 50 Ω termination ($i = 20mA$), $E_{I_{local}} + E_{I_{global}} = 35mV/m$ at a probe distance of 1 mm. This translates to an electric field of $E_I \approx 6mV/m$ for our case with an AES peak current $i_{AES_{max}} = 3.2mA$. Using Eqn. 15, we obtain $E_{I_{local}} = \frac{1}{25} * 6 = 0.24mV/m$ and $E_{I_{global}} = \frac{24}{25} * 6 = 5.76mV/m$.

As the ASNI circuit is embedded on top of the AES-128 encryption engine, using Eqns. 12, 13, 14 the measured electric field becomes $E_{I_{ASNI}} = \frac{0.24}{20} + \frac{5.76}{200} \approx 0.04mV/m$, which means that the effective suppression of the AES signature is $\sim 150\times$.

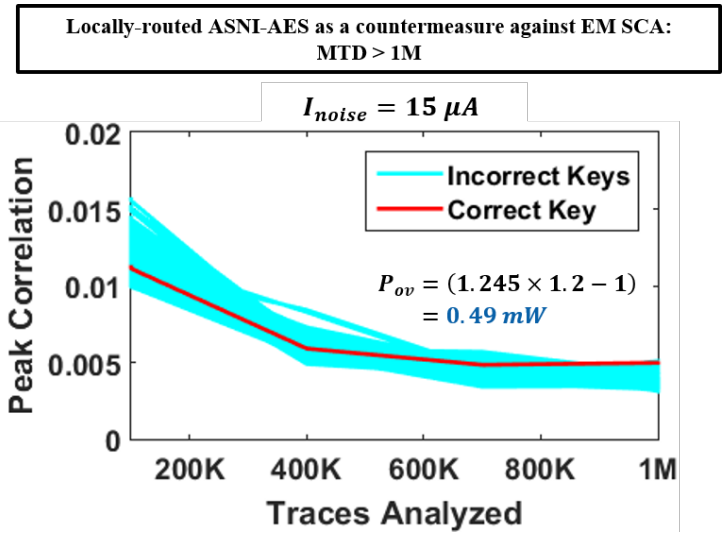

Figure 17: Locally-routed ASNI-AES: Noise Injection on the modified AES in Attenuated Signature domain, to achieve MTD of 1 Million traces.

6.1 Results & Overhead Comparison

We perform CEMA attack on the AES-128 core with a clock frequency of 40 MHz and an average current ($I_{AES_{avg}}$) of $\sim 1mA$ (peak current = 3.2 mA). The CEMA attack reveals the secret key of the unprotected AES within $< 1K$ traces (Figure 4), whereas the same attack on the ASNI-AES does not reveal the secret key even with $1M$ traces.

As the ASNI-AES core is subjected to a CEMA attack, Figure 17 shows that only $15\mu A$ of noise current injection is required to achieve Minimum Traces to Disclosure (MTD) $> 1M$. The current consumed by the amplifier in the shunt LDO loop consumes a current of $\sim 100\mu A$ and hence the total overhead current is given as $I_{ov} = I_{bleed} + I_{noise} + I_{opamp} = 130\mu A + 15\mu A + 100\mu A \approx 0.24mA$. Thus the total overhead power for the ASNI-AES architecture is $(1.13mA + 0.015mA + 0.1mA) * 1.2V - 1mA * 1V = 0.49mW$.

Power efficiency for ASNI-AES is given as, $\eta = \frac{(1mA*1V)}{(1.245mA*1.2V)} * 100 \approx 67\%$ (includes noise overhead). Hence, ASNI-AES consumes similar overhead as [18], but does not incur the performance penalty. Implementation of the SAH in 130 nm technology consumes an area of $\sim 0.08mm^2$, while a standalone AES incurs $0.35mm^2$, which implies an area overhead of $\sim 22.85\%$.

7 Conclusion

Electromagnetic emission from cryptographic ICs is a prominent side-channel attack vector to extract the secret key without physical access to the device. The growth of internet-connected small form-factor devices and the availability of cheap commercial EM probes calls for an efficient countermeasure against EM SCA. This paper, for the first time, performs a white-box modeling of the interconnect metal-via stack within an integrated circuit which leaks critical signal transitions in the form of EM radiation. System-level modeling of the interconnect structure for Intel 32 nm CMOS process reveals that metals above layer 8 leak the most and can be detectable using commercially available cheap EM probes. The AES-128 encryption engine is locally routed in the lower-level metal layers and also encapsulated within a low-overhead signature suppression hardware (ASNI). The ASNI circuit is then routed to the leaky higher-level metals, which now contains only the

suppressed AES signatures. Hence, local low-level metal routing along with the ASNI as a efficient shield protects the AES-128 encryption signatures from radiating, thereby achieving an $MTD > 1M$ with only a tiny noise injection of $15\mu A$. Low-level metal routing technique along with the ASNI encapsulation not only provides a low-overhead solution (1.5× power, 1.23× area overhead) against EM SCA, but it is also a generic countermeasure and can be extended to other cryptographic engines.

Acknowledgement

This work was supported in part by Intel Corporation, and in part by the National Science Foundation (NSF) under Grant CNS 17-19235. The authors would like to thank Mr. Shovan Maity for his constructive feedback which helped improve the quality of this paper.

References

[AARR02] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side—Channel(s). In *Cryptographic Hardware and Embedded Systems - CHES 2002*, Lecture Notes in Computer Science, pages 29–45. Springer, Berlin, Heidelberg, August 2002.

[Bal16] Constantine A. Balanis. *Antenna Theory: Analysis and Design*. Wiley, Hoboken, NJ, 4th edition, February 2016.

[BB03] David Brumley and Dan Boneh. Remote Timing Attacks Are Practical. In *Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12*, SSYM'03, pages 1–1, Berkeley, CA, USA, 2003. USENIX Association.

[BCO04] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, number 3156 in Lecture Notes in Computer Science, pages 16–29. Springer Berlin Heidelberg, August 2004.

[BGLT06] Marco Bucci, Luca Giancane, Raimondo Luzzi, and Alessandro Trifiletti. Three-Phase Dual-Rail Pre-charge Logic. In *Cryptographic Hardware and Embedded Systems - CHES 2006*, Lecture Notes in Computer Science, pages 232–241. Springer, Berlin, Heidelberg, October 2006.

[CEM18] Thomas De Cnudde, Maik Ender, and Amir Moradi. Hardware Masking, Revisited. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(2):123–148, May 2018.

[DMN+17] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 62–67, May 2017.

[DMN+18] 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 Transactions on Circuits and Systems I: Regular Papers*, pages 1–12, 2018.

[GM11] Tim Güneysu and Amir Moradi. Generic Side-Channel Countermeasures for Reconfigurable Devices. In *Cryptographic Hardware and Embedded Systems – CHES 2011*, Lecture Notes in Computer Science, pages 33–48. Springer, Berlin, Heidelberg, September 2011.

[GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *Cryptographic Hardware and Embedded Systems — CHES 2001*, Lecture Notes in Computer Science, pages 251–261. Springer, Berlin, Heidelberg, May 2001.

[GPPT15] Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation. In *Cryptographic Hardware and Embedded Systems – CHES 2015*, Lecture Notes in Computer Science, pages 207–228. Springer, Berlin, Heidelberg, September 2015.

[GPPT16] Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs. Technical Report 129, 2016.

[Gri17] David J. Griffiths. *Introduction to Electrodynamics*. Cambridge University Press, Cambridge, United Kingdom ; New York, NY, 4th edition, July 2017.

[GST14] Daniel Genkin, Adi Shamir, and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. In *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, pages 444–461. Springer, Berlin, Heidelberg, August 2014.

[HHM+14] Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki. EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor. In *Cryptographic Hardware and Embedded Systems – CHES 2014*, Lecture Notes in Computer Science, pages 1–16. Springer, Berlin, Heidelberg, September 2014.

[HTH+06] D. D. Hwang, K. Tiri, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede. AES-Based Security Coprocessor IC in 0.18-um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks. *IEEE Journal of Solid-State Circuits*, 41(4):781–792, April 2006.

[KJJ99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, number 1666 in Lecture Notes in Computer Science, pages 388–397. Springer Berlin Heidelberg, August 1999.

[KSM+17] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay. 8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator. In *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 142–143, February 2017.

[KSYO17] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky. Efficient simulation of EM side-channel attack resilience. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 123–130, November 2017.

[LCC+06] Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson, Christine Servière, and Jean-Louis Lacoume. A Proposition for Correlation Power Analysis Enhancement. In *Cryptographic Hardware and Embedded Systems - CHES 2006*, Lecture Notes in Computer Science, pages 174–186. Springer, Berlin, Heidelberg, October 2006.

[LMPT15] J. Longo, E. De Mulder, D. Page, and M. Tunstall. SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip. In *Cryptographic Hardware and Embedded Systems – CHES 2015*, Lecture Notes in Computer Science, pages 620–640. Springer, Berlin, Heidelberg, September 2015.

[LMT+09] Victor Lomné, Philippe Maurine, Lionel Torres, Michel Robert, Rafael Soares, and Ney Calazans. Evaluation on FPGA of Triple Rail Logic Robustness Against DPA and DEMA. In *Proceedings of the Conference on Design, Automation and Test in Europe*, DATE '09, pages 634–639, 3001 Leuven, Belgium, Belgium, 2009. European Design and Automation Association.

[MBO+05] E. De Mulder, P. Buysschaert, S. B. Ors, P. Delmotte, B. Preneel, G. Vandenbosch, and I. Verbauwhede. Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem. In *EUROCON 2005 - The International Conference on "Computer as a Tool"*, volume 2, pages 1879–1882, November 2005.

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer US, 2007.

[NAB+08] S. Natarajan, M. Armstrong, M. Bost, R. Brain, M. Brazier, C. H. Chang, V. Chikarmane, M. Childs, H. Deshpande, K. Dev, G. Ding, T. Ghani, O. Golonzka, W. Han,

J. He, R. Heussner, R. James, I. Jin, C. Kenyon, S. Klopcic, S. H. Lee, M. Liu, S. Lodha, B. McFadden, A. Murthy, L. Neiberg, J. Neirynck, P. Packan, S. Pae, C. Parker, C. Pelto, L. Pipes, J. Sebastian, J. Seiple, B. Sell, S. Sivakumar, B. Song, K. Tone, T. Troeger, C. Weber, M. Yang, A. Yeoh, and K. Zhang. A 32nm logic technology featuring 2nd-generation high-k + metal-gate transistors, enhanced channel strain and 0.171 um2 SRAM cell size in a 291mb array. In *2008 IEEE International Electron Devices Meeting*, pages 1–3, December 2008.

[O'F17] Colin O'Flynn. A Framework for Embedded Hardware Security Analysis. July 2017.

[OLS+08] Thomas Ordas, Mathieu Lisart, Etienne Sicard, Philippe Maurine, and Lionel Torres. Near-Field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits. In *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*, Lecture Notes in Computer Science, pages 229–236. Springer, Berlin, Heidelberg, September 2008.

[OZ14] Colin O'Flynn and Chen Zhizhang. ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research, 2014.

[PAA+09] P. Packan, S. Akbar, M. Armstrong, D. Bergstrom, M. Brazier, H. Deshpande, K. Dev, G. Ding, T. Ghani, O. Golonzka, W. Han, J. He, R. Heussner, R. James, J. Jopling, C. Kenyon, S-H. Lee, M. Liu, S. Lodha, B. Mattis, A. Murthy, L. Neiberg, J. Neirynck, S. Pae, C. Parker, L. Pipes, J. Sebastian, J. Seiple, B. Sell, A. Sharma, S. Sivakumar, B. Song, A. St. Amour, K. Tone, T. Troeger, C. Weber, K. Zhang, Y. Luo, and S. Natarajan. High performance 32nm logic technology featuring 2nd generation high-k + metal gate transistors. pages 1–4. IEEE, December 2009.

[PSQ07] Eric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Power and electromagnetic analysis: Improved model, consequences and comparisons. *Integration, the VLSI Journal*, 40(1):52–60, January 2007.

[QS01] Jean-Jacques Quisquater and David Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In *Smart Card Programming and Security*, Lecture Notes in Computer Science, pages 200–210. Springer, Berlin, Heidelberg, 2001.

[RBN+15] Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, and Ingrid Verbauwhede. Consolidating Masking Schemes. In *Advances in Cryptology – CRYPTO 2015*, Lecture Notes in Computer Science, pages 764–783. Springer, Berlin, Heidelberg, August 2015.

[SKR+16] A. Singh, M. Kar, A. Rajan, V. De, and S. Mukhopadhyay. Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 145–148, May 2016.

[Sol] Tekbox Digital Solutions. Tekbox EMC Near-field Probes Manual.

[TAV02] K. Tiri, M. Akmal, and I. Verbauwhede. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Proceedings of the 28th European Solid-State Circuits Conference*, pages 403–406, September 2002.

[TB10] C. Tokunaga and D. Blaauw. Securing Encryption Systems With a Switched Capacitor Current Equalizer. *IEEE Journal of Solid-State Circuits*, 45(1):23–31, January 2010.

[YK17] W. Yu and S. Köse. A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(11):2934–2944, November 2017.

[YTK+10] M. Yamaguchi, H. Toriduka, S. Kobayashi, T. Sugawara, N. Hommaa, A. Satoh, and T. Aoki. Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis. In *2010 IEEE International Symposium on Electromagnetic Compatibility*, pages 103–108, July 2010.