cryptography

MDPI

Article

Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach

Debayan Das* and **Shreyas Sen**

Department of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, USA; shreyas@purdue.edu

* Correspondence: das60@purdue.edu

Received: 1 October 2020; Accepted: 29 October 2020; Published: 31 October 2020

Abstract: Electromagnetic and power side-channel analysis (SCA) provides attackers a prominent tool to extract the secret key from the cryptographic engine. In this article, we present our cross-device deep learning (DL)-based side-channel attack (*X-DeepSCA*) which reduces the time to attack on embedded devices, thereby increasing the threat surface significantly. Consequently, with the knowledge of such advanced attacks, we performed a ground-up white-box analysis of the crypto IC to root-cause the source of the electromagnetic (EM) side-channel leakage. Equipped with the understanding that the higher-level metals significantly contribute to the EM leakage, we present *STELLAR*, which proposes to route the crypto core within the lower metals and then embed it within a current-domain signature attenuation (CDSA) hardware to ensure that the critical correlated signature gets suppressed before it reaches the top-level metal layers. CDSA-AES256 with local lower metal routing was fabricated in a TSMC 65 nm process and evaluated against different profiled and non-profiled attacks, showing protection beyond $1B$ encryptions, compared to $\sim 10K$ for the unprotected AES. Overall, the presented countermeasure achieved a $100\times$ improvement over the state-of-the-art countermeasures available, with comparable power/area overheads and without any performance degradation. Moreover, it is a generic countermeasure and can be used to protect any crypto cores while preserving the legacy of the existing implementations.

Keywords: power/EM side-channel analysis attack; current domain signature attenuation hardware; low-overhead; deep-learning attack; *STELLAR*; *SCNIFFER*; *X-DeepSCA*; generic countermeasure

1. Introduction and Motivation

Over the last decade, we have witnessed a steady expansion of Internet-connected devices, and they are projected to proliferate even further [1]. As these devices remain inter-connected, it becomes important to protect even the weakest links in the network. Typically, the resource-constrained small form-factor edge devices are the most vulnerable points of attack in an IoT system. Hence, it becomes extremely important to employ cryptographic algorithms to ensure data security and confidentiality for all electronic devices. However, as these mathematically-secure crypto algorithms are implemented on a physical platform, they leak critical correlated information in the form of power consumption, electromagnetic (EM) emissions, cache hits/misses, timing and so on, leading to side-channel analysis (SCA) attacks, allowing an attacker to extract the secret key from the device. In this article, we focus on the power and EM SCA attacks.

Recently, embedded devices running a crypto core in a trusted execution environment (TEE) or secure proprietary enclaves have been shown to be vulnerable to the power SCA attacks [2]. The Cortex-M device under attack lacked a full cache and hence a cache-based timing attack could not

be performed. However, the on-board ADC (not in the secure zone/TEE) of the device could sense the power side-channel leakage which could then be exploited to mount a remote power attack on the AES accelerator [2].

Remote power SCA has been exploited on multi-tenant FPGAs, where one FPGA can be used to monitor the power consumption of another FPGA sharing the same power rails [3]. Additionally, sensing the change in frequency of a ring oscillator (RO) can provide useful information regarding the bit being processed on the sensitive bus [4]. Camurati et al. demonstrated a far-field EM SCA attack from 10 m on an ARM mbedTLS implementation [5]. Recently, the smart lighting system Philips Hue housing Atmel microcontrollers was hacked by exploiting the underlying operating system (OS), utilizing power side-channels [6]. Another recent distributed denial-of-service (DDoS) attack was demonstrated by the Dyn DNS company utilizing power SCA, taking control over millions of inter-connected webcams [7].

These real-world exploits only show a small subset of the wide range of vulnerabilities existing in many of the commercial resource-constrained edge devices. Hence, it becomes very critical to protect against these attack vectors pro-actively during the design phase itself. Hence, security considerations including the power and EM side-channel leakage analysis should form an integral part of the design life-cycle of the device. However, keeping in mind the resource constraints of the devices, we need to develop low-overhead countermeasures against both EM and power SCA attacks. Additionally, from an industry point of view, in order to reduce the time-to-market, we need generic and technology-scalable solutions. It is important for the countermeasure to be generic for industry to preserve its legacy implementations and have the countermeasure circuit as a wrapper around the crypto core. Additionally, technology scaling is very important to reduce the design effort.

In this article, we develop a generic low-overhead EM and power SCA countermeasure utilizing ground-up white-box analysis, and show the upcoming works leading toward a fully-synthesizable solution. Additionally, we will present the development of advanced cross-device deep-learning-based SCA attacks. These new attack vectors increase the threat surface of the embedded devices significantly, and hence it is prudent to evaluate the proposed countermeasure against such advanced attacks.

2. Background and Related Works

2.1. EM and Power SCA Attacks

Power and EM side-channels have been around for almost two decades now [8,9]. A power SCA attack typically requires the insertion of a small resistor ($\sim$0.5–10 Ω) in series with the power supply of the device that measures the voltage drop across it. On the other hand, EM SCA attacks are non-invasive and do not require any modification of the device under attack. With the improvement in sensitivity of commercially-available EM probes, EM attacks are becoming increasingly powerful. Recently, Fox IT demonstrated breaking an AES-256 crypto core in just five minutes from a 1 m distance [10]. The complexity of breaking an AES-256 is reduced from 2^{256} for brute-force attacks to 2^{13} for EM/power SCA. Additionally, transitioning from AES-128 to AES-256 only increases the SCA resilience linearly by a factor of 2$\times$, unlike the exponential increase in mathematical security.

2.1.1. Non-Profiled SCA Attack

For performing a power/EM side-channel attack, firstly, traces are collected using an oscilloscope or an ADC, while an encryption/crypto operation is performed, as shown in Figure 1. The attack can be plaintext (PT) in which case the attacker requires full control of the device under attack, or it can be a known ciphertext (CT), attack which is more practical since the CT is public. Next, depending on the point of attack for the specific target crypto algorithm and the platform it is running (software/hardware implementation), the attack model—either hamming weight (HW) or hamming distance (HD)—is chosen. Finally, multiple traces are analyzed and correlated against the HW/HD model and the correct key byte emerges out (Figure 1). Note that the attack is performed one byte at a

time for the case of AES (could be word-wise for another algorithm such as SHA), since the internal operations are byte-wise instead of the full 128 bits or 256 bits at a time for efficiency reasons. This is what is known as the correlational power/EM analysis (CPA/CEMA) attack [11]. These are direct attacks on the target device and are classified as the traditional non-profiled SCA attacks.

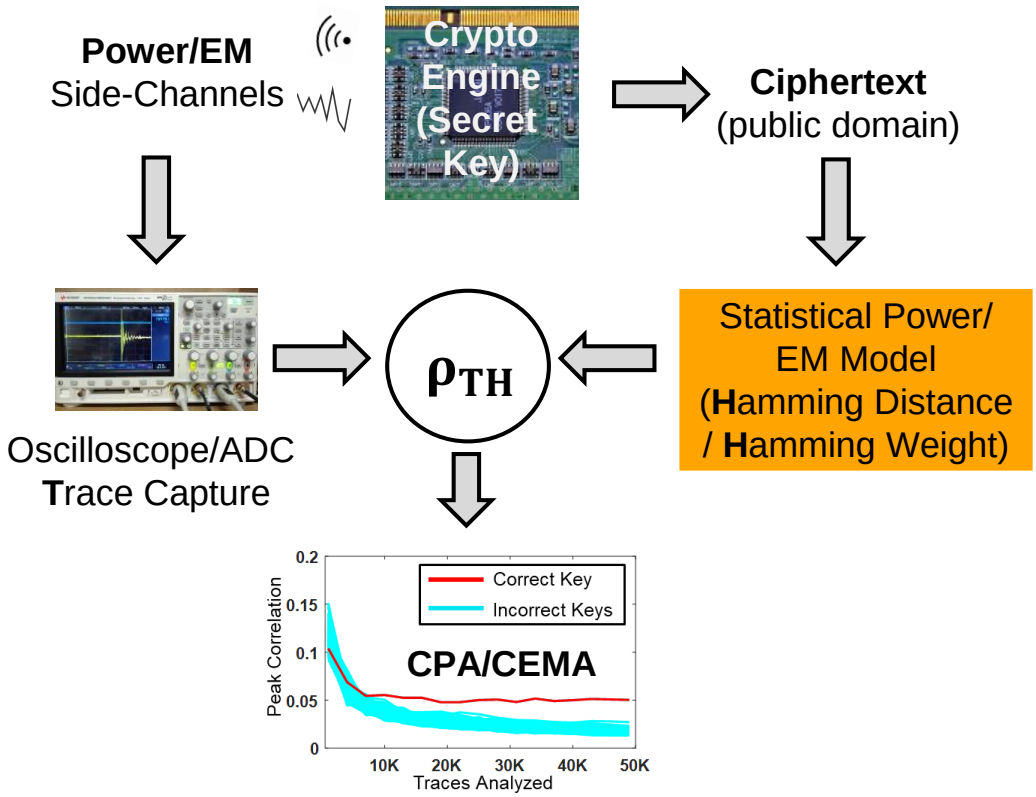


Figure 1. Power/electromagnetic (EM) side-channel analysis (SCA) attack set-up: Power/EM traces are collected from the crypto engine using an oscilloscope/ADC for a set of known ciphertexts (or chosen plaintexts) and then a hamming distance/weight (HD/HW) model is used for correlational analysis. After multiple traces are analyzed, the correct key (byte) emerges out.

2.1.2. Profiled SCA Attack

On the other hand, profiled SCA attacks are more powerful attacks and break the crypto implementations with far fewer traces compared to CPA/CEMA. It requires building an offline template using an identical device (phase 1), and then the attack is performed on a similar but unseen device. For this attack, all the heavy-lifting is offloaded to the training phase where the model learns the leakage patterns for the different key bytes. As seen from Figure 2, the profiled attacks can be classified as Gaussian template attacks (TAs) and the machine learning (ML) attack.

The TA uses multi-variate statistics to form the template by finding the points of interest (PoI) using the differences of means or the sum of absolute/squared differences. Once the template is formed, it can be used to perform an attack on an unseen device with as little as a single trace [12].

As shown in Figure 3, ML SCA evolved quite recently in 2011 [13]. The ML attacks use supervised techniques, such as the support vector machine (SVM), self-organizing maps (SOMs), random forest (RF) and deep neural networks (DNNs) to learn the leakage information from the training device. Once the model is trained, it can be used to break the secret key of an identical device. Figure 4 shows the evolution of the ML SCA class of attacks, leading towards deep learning (DL) attacks, which is a growing area of research today.

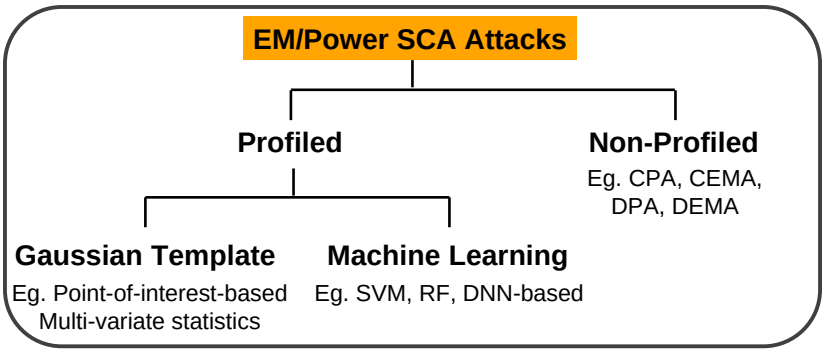


Figure 2. Classification of EM and power SCA attacks.

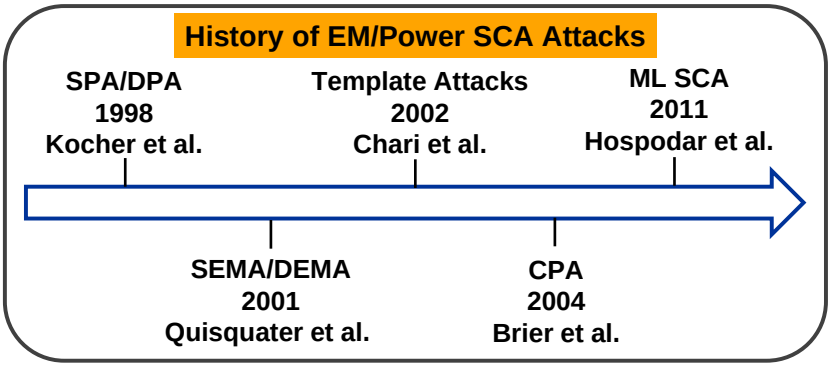


Figure 3. Evolution of EM and power SCA attacks over the last two decades since their inception in 1998 [8].

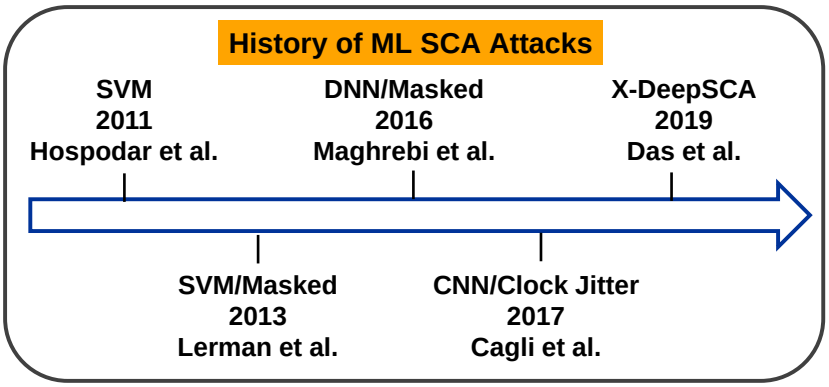


Figure 4. Evolution of machine learning-based SCA attacks. Starting with support vector machine (SVM) classifier attacks in 2011 [13], the side-channel research community began focusing on improving deep-learning (DL) SCA attacks. In 2019, we demonstrated the first cross-device deep-learning attack (*X-DeepSCA*), showing the feasibility of single-trace attacks.

As shown in Figure 4, SVMs were first utilized for ML SCA in 2011 by Hospodar et al. [13], followed by ML attacks on masked AES (DPA contest v4) by Lerman et al. [14] in 2015. The deep neural network (DNN)-based attack was first introduced by Maghrebi et al. in 2016 [15]. Cagli et al. used a convolutional neural network (CNN) to break a crypto implementation with clock misalignment [16], demonstrating that CNNs were capable of breaking time-domain obfuscation-based countermeasures. Compared to the statistical TA attacks, DNNs are widely preferred, as they can handle the higher dimensionality of the traces, and attacks can be fully-automated without the need for pre-processing techniques. However, until recently, most of these ML attacks only focused on training and testing the model on the same device on which the model was built. Recently, in DAC 2019, we demonstrated the

first cross-device deep-learning side-channel attack (*X-DeepSCA*) on AES-128 [17], showing the feasibility of single-trace attacks, thereby enhancing the threat surface of the embedded devices significantly.

2.2. State-of-the-Art Countermeasures

Countermeasures against EM/power SCA can be classified as logical, architectural and physical (circuit-level) countermeasures (Figure 5). Most of the logical and architectural countermeasures are design and algorithm-specific, while the circuit-level countermeasures are generic to any crypto algorithm and can be used as a wrapper around it. All of these countermeasures operate on the fundamental principle of decreasing the signal-to-noise ratio (SNR), and thus rely on the combination of two key techniques: (i) noise injection (NI), and (ii) critical correlated signature suppression.

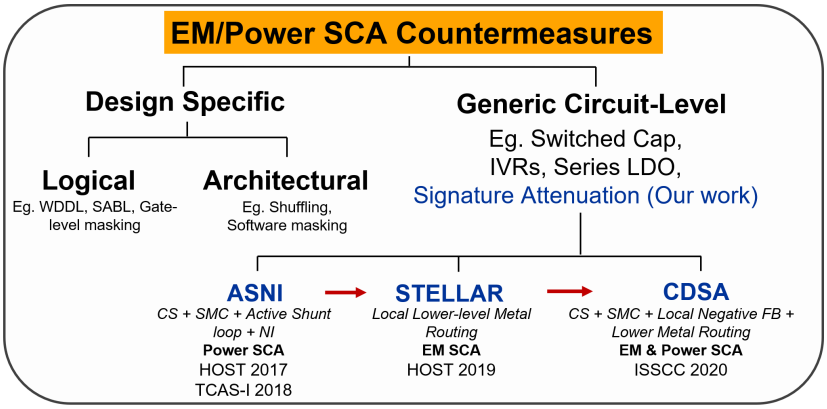


Figure 5. Classification of the EM/power SCA countermeasures. Logical and architectural countermeasures are design-specific, while the physical circuit-level countermeasures are generic to any crypto implementation. Our work on signature attenuation with local lower metal routing has evolved over the years, starting with attenuated signature noise injection (ASNI) [18,19], moving on to STELLAR (signature attenuation embedded crypto with low-level metal routing) [20,21] and finally reaching the chip-level implementation on a form of CDSA (current domain signature attenuation) [22].

2.2.1. Logical Countermeasures

Logical countermeasures are mainly based on power balancing which include the wave dynamic differential logic (WDDL) [23], dual-rail pre-charge (DRP) circuits, sense amplifier based logic (SABL) and gate-level masking [24]. Dual-rail logic requires custom design of the logic gates to equalize the power consumption. In DRP cells, one of the outputs always switches its state (either the original output or its compliment), making the power consumption constant. SABL employs a dynamic and differential logic and requires the complete re-design of the standard cell library to ensure that all the four output transitions (0-0, 0-1, 1-0, 1-1) consume the same amount of power. WDDL appears to be the first protection technique validated in silicon and can be built using the single-rail standard library cells; however, it incurs a 3× area overhead, a 4× power overhead and a 4× performance degradation.

2.2.2. Architectural Countermeasures

Architectural countermeasures introduce amplitude or time distortions to obfuscate the power/EM trace. Time distortion is achieved by random insertion of dummy operations or by shuffling the operations. However, it does not provide high levels of protection (minimum traces to disclosure or MTD) as the number of operations that can be shuffled is limited depending on the specific algorithm and its architecture. Additionally, clock skipping and dynamic voltage and frequency scaling (DVFS)-based countermeasures have been shown to be defeated using advanced attacks [25]. Algorithmic masking techniques are commonly used [26], but they incur $> 2\times$ area and power overheads.

Overall, the logical and architectural countermeasures explored till date, including the masking and hiding techniques, suffer from high area/power/throughput overheads and are specific to a crypto algorithm. Next, we will study the generic countermeasures that are applicable to any crypto algorithms.

2.2.3. Circuit-Level Physical Countermeasures

This class of countermeasures involve physical noise injection (NI) and supply isolation circuits. While NI has been used extensively in many countermeasures, NI alone suffers from large power and area overheads. Supply isolation techniques include the switched capacitor current equalizer [27], the integrated voltage regulator (IVR) [28] and series low-dropout (LDO) regulators [29]. The switched capacitor current equalizer-based countermeasure is a novel technique and achieves high MTD, but suffers from multiple trade-offs leading to a 2× performance degradation. IVRs using buck converters and series LDOs have been explored extensively; however, they suffer from large passives—inductors and on-chip capacitors. As we will discuss later, these on-chip MIM (metal–insulator–metal) capacitors can leak critical side-channel information through the higher-level metal layers in the form of EM leakage [20,22]. Additionally, a series LDO-based implementation inherently leaks critical correlated information [19], as it instantaneously tracks the voltage fluctuations across the crypto core and regulates the current accordingly. Hence, we need a generic countermeasure for both power and EM attacks with low overheads, and we can only achieve it by understanding the root-cause of the side-channel leakage from the IC, which we will discuss in the upcoming sections.

In the next section, we will discuss the *X-DeepSCA* attack in detail. In Section 4, we present SCNIFFER which is a low-cost, fully-automated end-to-end EM SCA attack framework. Section 5 demonstrates our work on the EM white-box analysis leading to STELLAR. In Section 6, the design of the current-domain signature attenuation (CDSA) hardware is presented along with the chip-level measurement results. Section 7 presents the evaluation of the CDSA hardware against deep-learning attacks. Finally, Section 8 concludes the paper along with future directions.

3. Cross-Device Deep-Learning Attack: *X-DeepSCA*

As discussed in the last section, prior works have focused on improving and evaluating the deep learning (DL)-based SCA attack on the same device which was used to train the deep neural network (DNN). The main challenge for a cross-device DL SCA attack is that the inter-device variations for the same key are significantly higher compared to the inter-key (inter-class) variations of the same device, as shown in Figure 6a [17]. This observation is fundamental to what makes cross-device attacks particularly challenging in a real-world scenario. Figure 6b shows the fully connected DNN utilized for the DL SCA attack on the AES-128 [17]. Confusion matrices in Figure 6c reveal that although the test accuracy on the same device is very high (red dots represent the misclassified key bytes), the test accuracy on a different but identical device is significantly lower. Hence, training with one device overfits to the traces from that particular device and may not necessarily generalize well to other identical devices.

Hence, in *X-DeepSCA* we propose the concept of multi-device training utilizing traces from multiple devices along with the proper choice of hyperparameters for the 256-class DNN. The DNN model with multi-device (four training devices) training achieves a *X-DeepSCA* accuracy of >99.9% for all the four different test devices (Figure 7c–f), leading to single-trace attacks. Figure 7a,b shows the individual class accuracies (in black) and the maximum mispredicted class (in red) for 1-device training and multi-device training respectively. We see that for the 1-device training in Figure 7a, the red and black curves overlap, while with multi-device training, there is a significant reduction in entropy (difference between the two curves), allowing *X-DeepSCA* attack to predict with high accuracy [17].

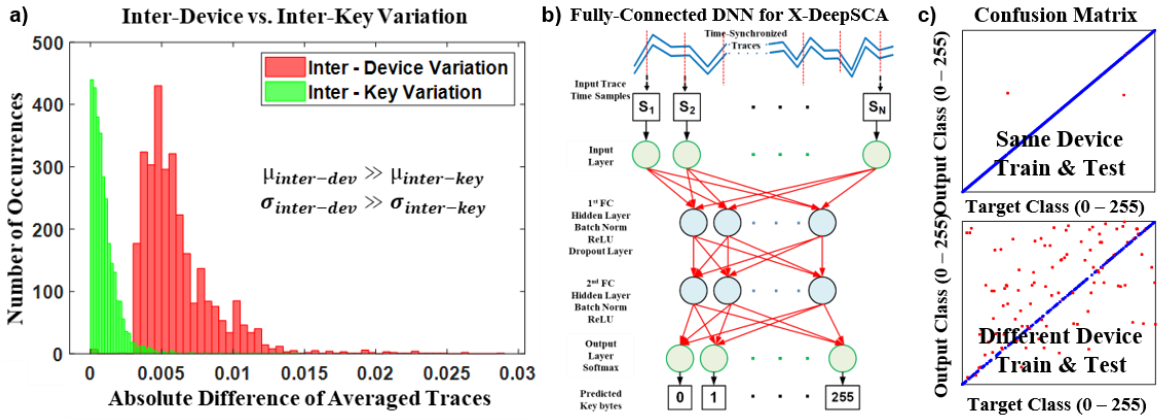


Figure 6. Motivation for the development of *X-DeepSCA* attack: (**a**) The inter-device variations for the same key are much higher compared to the inter-key variations of the same device, revealing the challenges in dealing with the issue of portability of these DL SCA attacks across devices [17]. (**b**) Fully-connected DNN architecture with 2 hidden layers and 256 output classes used for the *X-DeepSCA* attack [17]. (**c**) The confusion matrix plot shows that the test accuracy for the same device is significantly higher compared to the accuracy for a different device for the DNN model, showing the need for improvement in the domain of cross-device ML attacks.

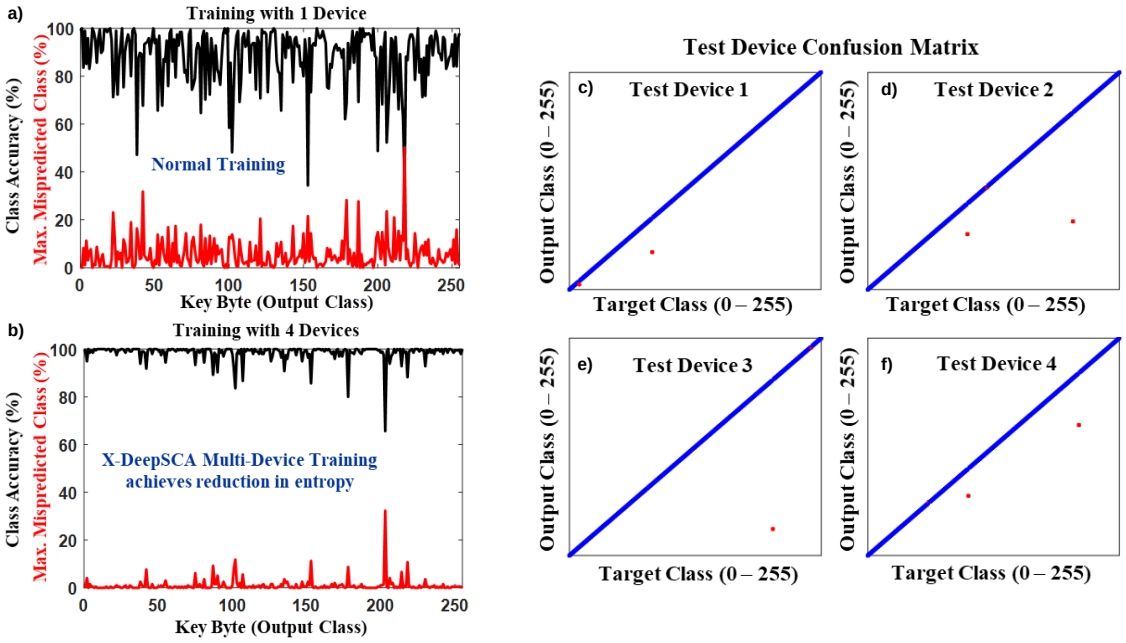


Figure 7. *X-DeepSCA* results: (**a**,**b**) Analysis of the individual class (key byte) distribution for 1-device and multi-device (4) training respectively. It can be seen that the entropy, that is, the distance between the red (maximum percentage of misprediction to a particular class, represents the bias of the DNN) and black curves (individual class accuracy), increases for the multi-device training, leading to higher accuracies for the *X-DeepSCA* attack. (**c**–**f**) Confusion matrices for the unseen test devices show significantly high accuracy (>99.9%) for the single-trace *X-DeepSCA* attacks.

Figure 8 shows that for different SNR scenarios, the proposed *X-DeepSCA* attack achieves ∼10× lower MTD, thereby increasing the threat surface significantly [17]. Additionally, a N-trace *X-DeepSCA* attack is able to break the secret key even if the model is trained with low accuracy for lower SNR traces [17]. Using the concept of majority voting, the success probability of an attacker can be >99.9%,

even when the model has a single-trace test accuracy of as low as ∼1% (for the 256-class identity model) using Equation (1).

$$\begin{aligned} Pr(Majority(N) = K_{target}) &= \sum_{x=2}^{N} Pr(x) \\ &= \sum_{x=2}^{N} \binom{N}{x} p^x (1-p)^{N-x} \frac{N-x}{255^{N-x}} \end{aligned} \tag{1}$$

where K_{target} is the target key byte, $Pr(Majority(N) = K_{target})$ gives the probability of successful target key recovery utilizing majority voting with N traces and p is the single-trace *X-DeepSCA* attack accuracy.

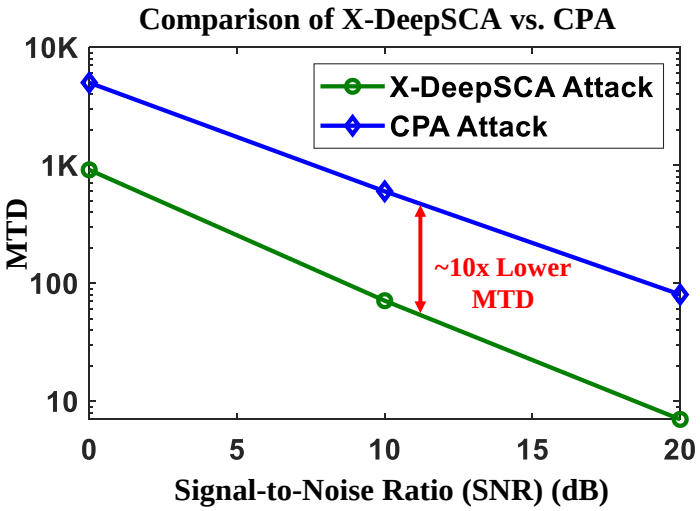


Figure 8. Across different levels of signal-to-noise ratio (SNR), the *X-DeepSCA* attack shows ∼10× lower minimum traces to disclosure (MTD) compared to the traditional correlational power attacks (CPA), enhancing the threat surface for embedded devices significantly.

To further enhance the effectiveness of *X-DeepSCA* attacks, pre-processing techniques such as principal component analysis (PCA) for dimensionality reduction and dynamic time warping (DTW) have been explored [30]. The code for the *X-DeepSCA* attack is shared publicly in GitHub [31].

In the next section, we will study the development of a low-cost fully-automated end-to-end EM SCA attack framework.

4. Low-Cost Automated EM SCA Attack Framework: *SCNIFFER*

Today, to perform an EM SCA attack on a device, the entire chip is manually scanned and the MTD analysis is performed at each point on the chip to reveal the secret key of the encryption algorithm. However, an automated end-to-end framework for EM leakage localization, trace acquisition and the attack has been missing. Recently, we proposed *SCNIFFER*, which is a low-cost, automated EM side-channel leakage sniffing platform to perform efficient end-to-end side-channel attacks [32]. Using a leakage measure such as test vector leakage assessment (TVLA), or the signal to noise ratio (SNR), we propose a greedy gradient-search heuristic that converges to one of the points of highest EM leakage on the chip (dimension: $N \times N$) within $O(N)$ iterations, and then performs correlational EM analysis (CEMA) at that point (Figure 9a). This reduces the CEMA attack time by $\sim N$ times compared to an exhaustive MTD analysis, and by $>20\times$ compared to choosing an attack location at random [32].

The set-up for the *SCNIFFER* framework is shown in Figure 9b. It uses a low-cost 3D printer as the EM scanner by mounting the H-probe on it and "sniffing" on the surface of a device under attack to quickly find the best position of EM leakage and then mount a CEMA at the point of maximum leakage. A demonstration video for *SCNIFFER* can be found in [33].

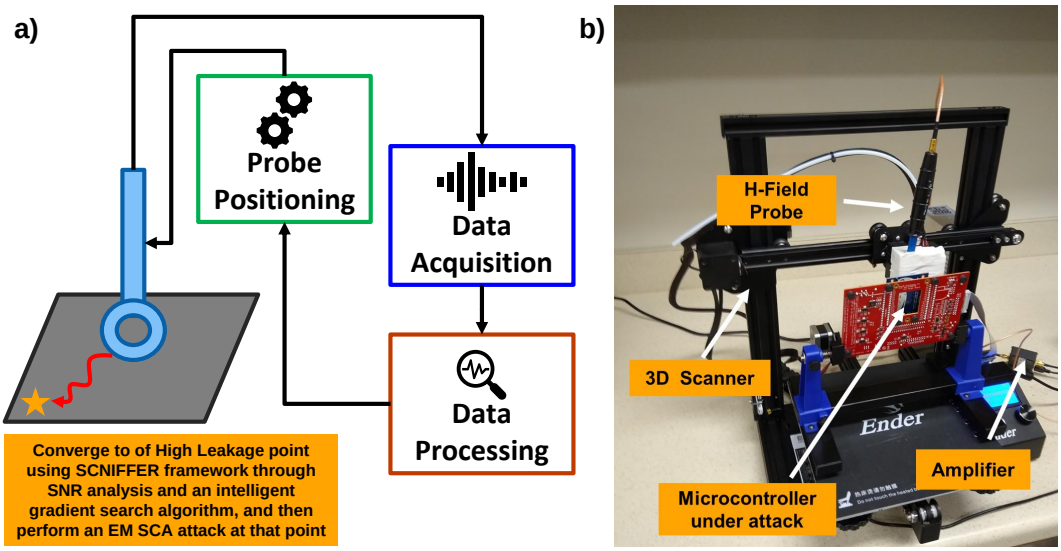


Figure 9. (**a**) *SCNIFFER* integrates the EM scanning, trace collection, intelligent fast localization and attack together, to enable an end-to-end EM SCA framework [32]. (**b**) Implementation of the low-cost *SCNIFFER* system with the 3D EM scanner, H-probe, amplifier, target device and chipwhisperer system for the trace capture.

Figure 10a shows the trajectory of the *SCNIFFER* framework as the EM probe scans the chip to reach to the point of highest leakage. Any leakage metric, such as the test vector leakage assessment (TVLA) or the signal to noise ratio (SNR), can be used, and the *SCNIFFER* platform will be able to converge to a location of high leakage in $O(N)$ measurements. Hence, compared to a exhaustive search, *SCNIFFER* reduces the traces required for an end-to-end attack by 100×, as shown in Figure 10b, by utilizing the intelligent gradient search algorithm based on TVLA or SNR assessment and then CEMA at the best point of leakage. Overall, the *SCNIFFER* framework can be used to attack any crypto implementation, and other profiling attacks like *X-DeepSCA* can also be used to perform the EM SCA attack instead of CEMA to further reduce the time to attack.

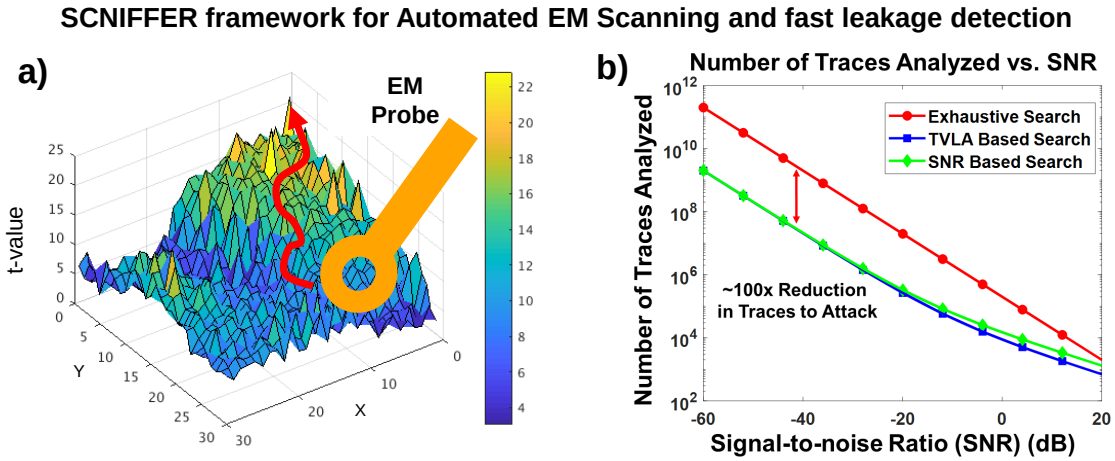


Figure 10. (**a**) A 3D TVLA surface plot of AES-128 for a 30x30 grid across the chip. *SCNIFFER* determines the maximum leakage point within 30 iterations (linear time) utilizing a gradient search heuristic instead of the traditional exhaustive search. Once the best leakage point on the chip is found, *SCNIFFER* uses CEMA to perform the EM SCA attack to recover the correct key. (**b**) *SCNIFFER* with SNR/TVLA-based intelligent gradient search shows a ∼100× reduction in the number of traces required for the end-to-end attack compared to the exhaustive search [32].

In this aspect, it is worth mentioning that *X-DeepSCA* attack has been demonstrated on the power traces, and translating the attack to EM traces may not be straightforward due to the high dimensionality of the EM traces. Hence, as part of the future works, it is important to build cross-device DL SCA attack models on the low SNR EM traces. Additionally, *X-DeepSCA* in the EM domain can be augmented with the *SCNIFFER* framework to provide even faster convergence and attacking.

In the next section, we will present our proposed countermeasures against EM and power SCA attacks through a ground-up root-cause analysis.

5. Countermeasure against EM SCA

Figure 11 shows the different layers of abstraction for the countermeasures. Both logical and architectural countermeasures are design-specific and incur high power/area/performance overheads; circuit-level countermeasures are generic and often have lower overheads since they are designed at the transistor level, which is the lowest layer of abstraction and forms the root of trust.

Most of the logical and architectural countermeasures suffer from high power, area and throughput overheads ($>2\times$). Although most of the circuit-level techniques are generic, they treat the crypto engine as a black box and hence incur high overheads (Figure 12). Our goal is to develop a white-box understanding of the EM leakage from a crypto IC leading towards a low-overhead generic countermeasure.

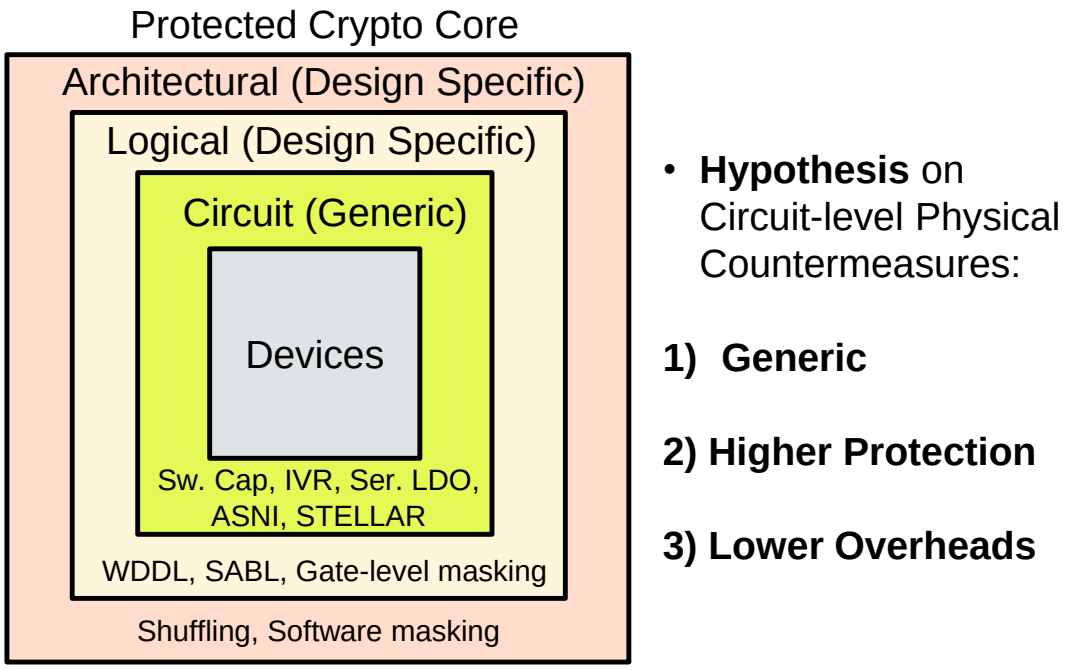
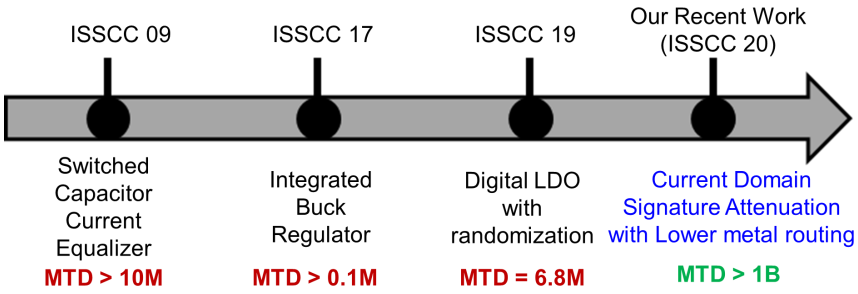


Figure 11. Different abstraction levels of the state-of-the-art countermeasures. Circuit-level solutions are closest to the root of trust (transistor-level) and hence would provide the lowest overhead and generic solutions. However, it would be very critical to understand the root-cause of the side-channels to develop a low-overhead generic countermeasure.

5.1. Ground-up Root-Cause Analysis of the EM Leakage

All crypto engines, such as AES256/SHA256/ECC, consist of multiple digital gates. These transistors create changing currents as they switch, leading to the EM radiation. Now, the main question arises—what does this generated EM field depend on? Is it caused by the transistors alone?



Technique	Switched Capacitor Current Equalizer	Integrated Buck Regulator	Digital LDO with Randomization	Current Domain Signature Attenuation
MTD	>10M	>0.1M	6.8M	>1B
Cap Ind	300pF None	3.2nF MIM 11.6nH (board)	1.9nF MIM None	150pF MOS None
Limitation	2x Perf. Deg.	On board Inductor → Attackable	High MIM cap → EM leakage	-

Figure 12. State-of-the-art circuit-level countermeasures include the switched capacitor current equalizer [27], integrated voltage regulator (IVR) [28] and series LDOs [29]. The table highlights depicts the main challenges with these countermeasures. In the next few sections, we will see how we achieved a 100× improvement in MTD over the previous works with comparable overheads.

Well, the EM fields depend on the metal layers and vias carrying the current, and not the transistors themselves. The transformation of the switching currents through the metal-interconnect stack creates the EM radiation, which is then picked up by an attacker, leading to EM SCA attacks. Higher metal layers are thicker (Figure 13a,b) and hence act as more efficient antennas at the operating frequency of the crypto cores, compared to the lower metal layers. Hence, the EM leakage from the top metal layers (M_9 and above for the Intel 32nm process [20]) has a higher probability of detection using the commercially available EM probes. This was proven using 3D FEM system-level simulations of the Intel 32 nm metal stack [20] (Figure 13c). Hence, our goal was not to pass the correlated crypto current through the high-level metal layers. However, it needs to connect to the external power pin. Thus, we somehow need to restrict the correlated power signatures to the lower-level metal layers, such that the EM leakage is suppressed locally.

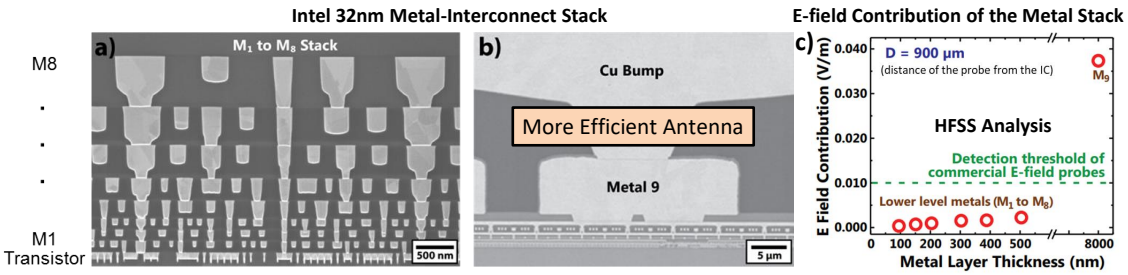


Figure 13. White-box modeling and analysis: (**a**) Intel 32 nm metal-interconnect stack, (**b**) the top-level metal layers and the copper bump are huge compared to the lower-level metal layers. (**c**) 3D FEM simulations performed in HFSS on the Intel 32nm metal stack reveal that the top metals M9 and above can be detected by the commercially available EM probes [20].

5.2. Local Lower Metal Routing: STELLAR

The observation that the correlated crypto signature should not be passed through the top metal layers led to the development of *STELLAR*, which stands for signature attenuation embedded crypto with low-level metal routing [20]. *STELLAR* proposes routing the crypto core within the lower metal layers and then embed it within a signature attenuation hardware (SAH) locally within the lower-level metals, such that the critical signature is significantly suppressed before it reaches the top metal layers, which radiate significantly. This idea of signature suppression within the lower-level metal layers is shown in Figure 14. The current from the crypto core (denoted by blue line) goes through the

SAH, which embeds the crypto core locally within the lower metals and then the attenuated signature is passed through the higher-level metal layers (denoted by green line) to connect to the external power pin.

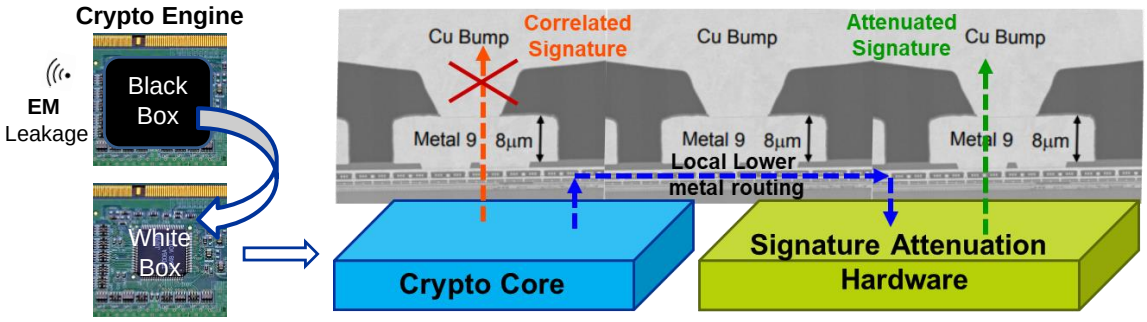


Figure 14. EM SCA countermeasure: With the white-box understanding of the EM leakage, we present *STELLAR*, which proposes to route the crypto core within the lower metal layers and then embed it within a signature attenuation hardware (SAH) which suppresses the correlated crypto signature significantly before it reaches the higher metal layers to connect to the external pins [20].

Our work on *STELLAR* led to the first white-box analysis and developed a better understanding of the root-cause of the EM leakage. Now, by combining signature attenuation hardware (SAH) with lower-level metal routing, we can develop a highly resilient countermeasure against both EM and power SCA attacks. The local routing is extremely critical to minimize long routing of the critical signals.

As part of future works, we plan to develop further understanding of the genesis of the EM leakage so that we can eliminate it even closer to its source. In the next section, we will analyze the design of our signature attenuation hardware (SAH) and combine it with our *STELLAR* technique to prevent both EM and power SCA attacks.

6. Current-Domain Signature Attenuation (CDSA) Hardware

In this section, we will study the details of the signature attenuation hardware (SAH). In 2017, we proposed the first concept of SAH design in the form of attenuated signature noise injection (ASNI) [18], ref. [19] to prevent power side-channel analysis (SCA) attacks, generic for all cryptographic algorithms, without any performance overheads.

Current-Domain Signature Attenuation (CDSA) Hardware

The progression of the signature attenuation hardware (SAH) is shown in Figure 5. In ASNI, the key idea was to embed the crypto engine within a signature attenuation hardware (SAH) such that the correlated critical crypto signature is highly suppressed at the power supply node, which an attacker can access, and then inject a tiny amount of noise into to protect against power SCA attacks. Next, *STELLAR* demonstrated the efficacy of local lower-level metal routing to prevent EM SCA attacks, as discussed in Section 5. Finally, we combine the concepts of signature attenuation from ASNI and the local lower metal routing from *STELLAR* leading to the current domain signature attenuation hardware (CDSA), which was demonstrated in a 65 nm test-chip at the ISSCC 2020 [22].

Let us now understand the design details of the signature attenuation hardware (SAH). The goal of developing a SAH is to have a constant supply current independent of the variations in the crypto current. The first thing that we can think of is a constant current source (CS). However, a constant CS cannot drive a variable current load (crypto engine). Hence, a load capacitor (C_L) is required to account for the differences in the current, as shown in Figure 15a. Now, a high bandwidth (BW) shunt LDO can be utilized to bypass any excess current through the bleed NMOS [19] whenever the supply current (I_{CS}) is more than the crypto current (I_{Crypto}) [19]. A low-BW digital switched mode control

(SMC) loop compensates for the process, voltage and temperature (PVT) variations, and sets the I_{CS} to a quantization level closest to the average crypto current ($I_{Crypto_{avg}}$) by turning on or off required number of CS slices, such that $I_{CS} = I_{Crypto_{avg}} + \Delta$. The quantization error in the supply current Δ is bypassed through the shunt bleed. In steady state, once the top CS current is equal to the average crypto current, the SMC loop is disengaged and the attenuation is thus given by the load capacitance and the output resistance of the CS stage, $AT = \omega C_L r_{ds}$ (Figure 15b). Now, the MTD is proportional to AT^2, which means that a higher output resistance of the CS stage (r_{ds}) can reduce C_L, lowering the area overhead for iso-attenuation (or iso-MTD) [18]. Hence, a cascode CS stage with very high output impedance was chosen so that the load capacitance can be significantly reduced.

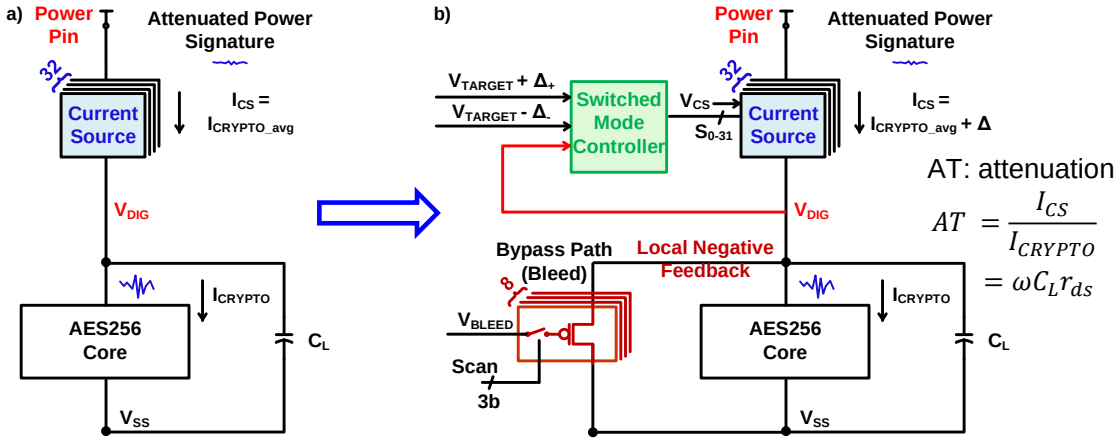


Figure 15. (**a**) In order to have a supply current independent of the crypto current, the first thing that comes to our mind is a constant current source (CS). An ideal implementation of the CS on top of the crypto engine is shown. However, this topology is highly unstable since it is difficult to maintain the exact average current through the CS. (**b**) Our proposed current-domain signature attenuation (CDSA) circuit ensures that the goal of high signature attenuation along with stability of the system is achieved by using a shunt bleed path and a low-bandwidth switched mode control loop which turns on or off the required number of CS slices [22].

During steady-state, the SMC loop is only engaged if the V_{reg} node voltage goes below $V_{target} - \Delta_-$ or is above $V_{target} + \Delta_+$, and remains disengaged as long as the voltage remains within the guard band. The low BW of the SMC loop ensures that the voltage fluctuations at the V_{reg} are not reflected instantaneously to the supply current, unlike series LDOs.

Current domain signature attenuation (CDSA) combines the signature attenuation hardware (SAH) from ASNI and the local lower metal routing from the *STELLAR* approach to develop the world's most secure SCA countermeasure with $<1.5\times$ area and power overheads [22]. The main difference in the SAH design is the replacement of the active shunt LDO loop with a biased PMOS bleed, as shown in Figure 15b. This reduces the power overhead while maintaining the same SCA security enhancement. The bleed PMOS provides the bypass path to drain the extra quantization error (Δ) in the CS current, and also provides an inherent local negative feedback (FB) allowing any average crypto current in between two quantized levels of the CS.

The cascode CS stage is designed such that the unit current per slice is higher than the key-dependent variation in $I_{Crypto_{avg}}$, so that the key-dependent information in the average crypto current is not transferred to the supply current and leaked by the bleed path, providing information-theoretic security [22,34].

CDSA-AES256 has been implemented in TSMC 65 nm technology (Figure 16) with local lower-metal routing up to M_6. The parallel AES-256 is encapsulated by the CDSA hardware, providing both EM and power SCA immunity.

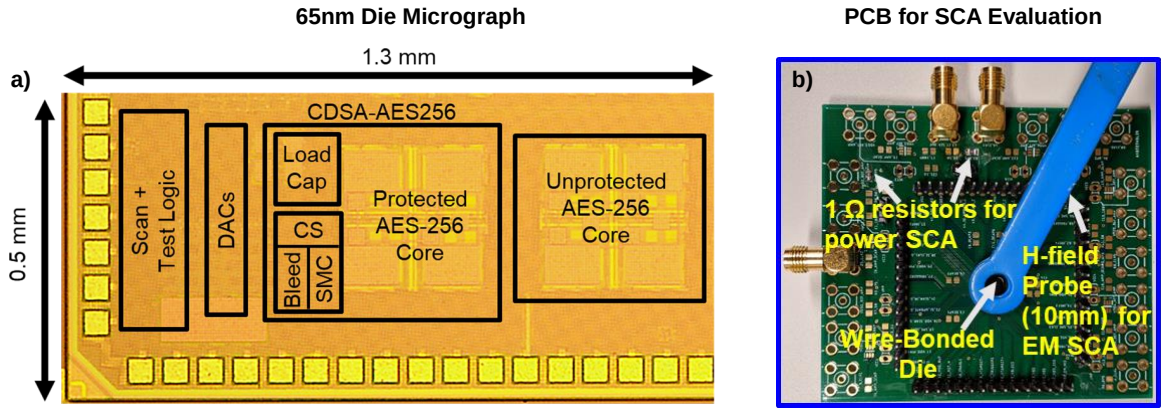


Figure 16. (**a**) Die micrograph of the system in 65 nm CMOS. The fabricated test chip contains both unprotected and protected AES-256. (**b**) PCB for power and EM SCA evaluation.

7. Measurement Results and Evaluation Metrics for Security and Overhead Comparison

The CDSA-AES256 testchip die photo is shown in Figure 16a, and the PCB for the power and EM SCA evaluation is shown in Figure 16b.

Measurements results of the CDSA-AES256 show an active signature attenuation of >350× (Figure 17a–e) for both power (Figure 17a,c) and EM traces (Figure 17d,e). In the intermediate V_{DIG} node across the AES, the 14 rounds of the AES are still visible; however, it is only kept in the testchip for debugging purposes and is not accessible to an external adversary.

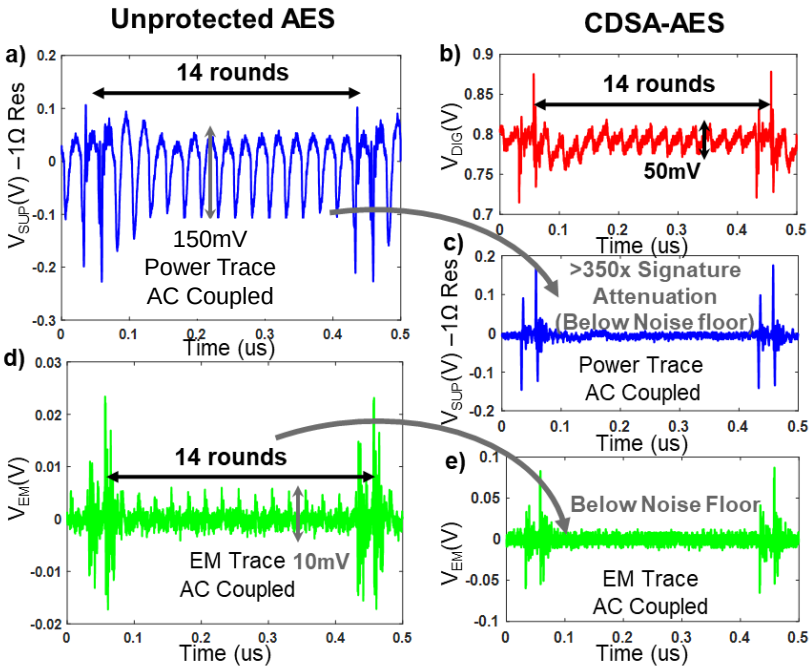


Figure 17. Time-domain measurements of the CDSA-AES: (**a**) For the unprotected AES, the power trace shows an amplitude of ∼150 mV, while (**c**) for the CDSA-AES256, the power trace remains below the noise floor, showing >350× active signature suppression. Similarly, for the EM traces (**d**,**e**), the 14 rounds of the AES are clearly visible for the unprotected implementation, while it remains below the noise floor for the CDSA-AES. (**b**) Although the V_{DIG} node across the AES shows the 14 rounds of the AES, it is only kept for debugging purposes and is not accessible to an attacker. It should be noted that we tolerate this ∼50 mV droop across the AES (due to lower load cap) and the high impedance CS on top ensures that the fluctuations are highly suppressed at the supply pin.

Both the unprotected and the protected AES implementations are now subjected to power and EM attacks. While the unprotected AES256 could be broken with only $8K$ and $12K$ traces respectively, for CPA and CEMA attacks, the protected CDSA-AES remains secure even after $1B$ encryptions (Figure 18a,b), showing an MTD improvement of 100× over the existing countermeasures [22]. The CPA and CEMA attacks were verified in the time and frequency domains. Finally, to evaluate the effects of the metal layers on the EM leakage, fixed vs. random test vector leakage analysis (TVLA) was performed. In Figure 18c, CDSA-AES256 with high-level metal routing showed an EM TVLA of ∼9, which is much higher than for the CDSA 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 improvement over the state-of-the-art is summarized in Figure 19. In terms of the MTD, which is the an important security metric in EM/power side-channel analysis, the proposed CDSA achieves 100× improvement over the previous works through signature attenuation and local lower metal routing. Other than the MTD, other important metrics are the area/power overheads. A detailed comparison with regard to the overheads in presented in the next section, along with the DL SCA attack evaluation.

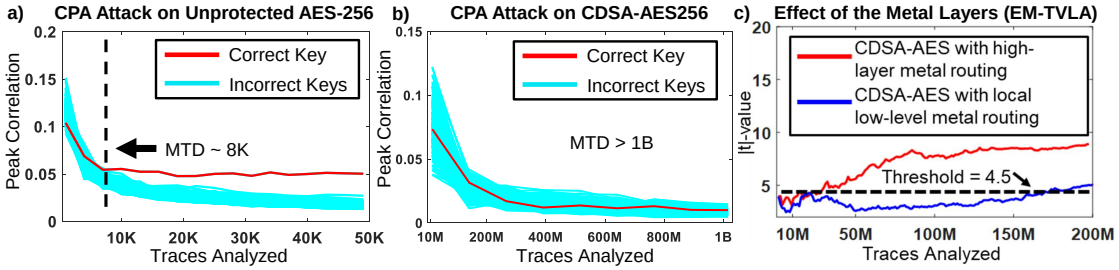


Figure 18. EM and power SCA attack evaluation. (**a**) CPA attack on the unprotected AES shows a MTD of $8K$, while (**b**) the CDSA-AES remains protected even after $1B$ traces are analyzed. (**c**) Effect of the metal layers on EM leakage is evaluated using test vector leakage analysis (TVLA). It can be seen that the CDSA-AES with higher metal routing has significantly higher leakage compared to the CDSA-AES with lower metal routing, proving for the first time the effect of metal routing on the EM side-channel leakage.

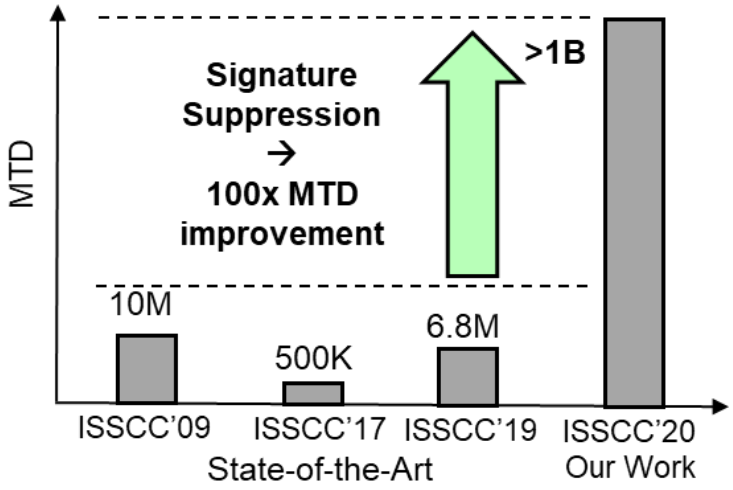


Figure 19. Summary: MTD comparison with the state-of-the-art countermeasures.

8. Evaluation of CDSA against DL SCA Attacks

The proposed CDSA is also evaluated against DNN-based profiling power SCA attacks [35]. A fully-connected DNN is used since the traces are time-aligned. As shown in Figure 20a, the DNN could be fully trained for the unprotected AES with only $5K$ traces, achieving a training and validation

accuracy of ∼99.9% within 10 epochs. The confusion matrix shown in Figure 20b reveals that the test accuracy remains >99.9% and the correct key byte can be accurately classified using a single trace.

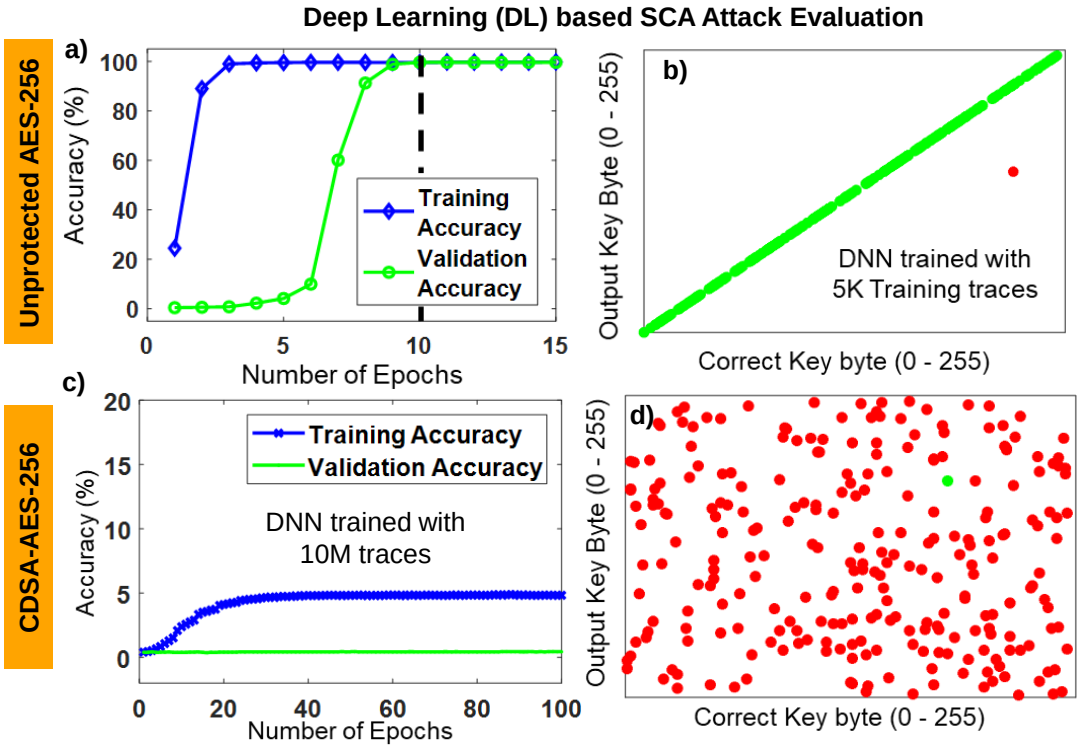


Figure 20. CDSA-AES256 evaluated against DL SCA attacks: (**a**,**b**) For the unprotected AES, the training and validation accuracy reaches ∼99.9% and the confusion plot reveals a test accuracy of >99.9% [35]. (**c**,**d**) Now, for the protected CDSA-AES256, the DNN could not be trained, even with 10*M* traces, showing the efficacy of the proposed countermeasure against these advanced DL SCA attacks.

On the other hand, for the protected CDSA-AES implementation, with a 350× signature attenuation, the DNN could not be trained, even after 10*M* power traces, demonstrating the efficacy of the proposed countermeasure.

As we discussed previously, many of the existing logical/architectural countermeasures used time-domain obfuscation through clock jitter or dummy insertion. The countermeasures of this type can be defeated by using convolutional neural networks (CNNs). However, CDSA attenuates the signature in the voltage domain and hence is a more fundamental solution.

9. Future Work and Conclusions

The ever-increasing growth of Internet-connected devices calls for improved security mechanisms to protect even the weakest points of entry in a network, which typically are the resource-constrained edge devices. This work presented the first cross-device deep-learning attack (*X-DeepSCA*), an end-to-end automated EM SCA attack framework in the form of *SCNIFFER* and the CDSA countermeasure to protect against all possible attacks through a ground-up root-cause analysis.

Overall, the CDSA achieved >1*B* EM/power SCA MTD against the non-profiled attacks, with 1.37× area and 1.49× power overhead (Figure 21) [22]. Figure 21 confirms the hypothesis that circuit-level countermeasures such as CDSA can provide the lowest overhead countermeasure with the highest security, as discussed in Figure 11. Leveraging signature attenuation along with local lower metal routing aided by the white-box analysis allowed us to achieve the best security ever reported in the literature (100× improvement compared to the prior works) with lower (or comparable) overheads than most of the previous countermeasures (Figure 21). It should be noted that it is a generic countermeasure and can be extended to any other crypto algorithm to protect against both

power and EM SCA without any performance degradation. Short demonstration videos for CDSA and *SCNIFFER* can be found in [33,36], respectively, and the data/code for *X-DeepSCA* is available publicly in GitHub [31].

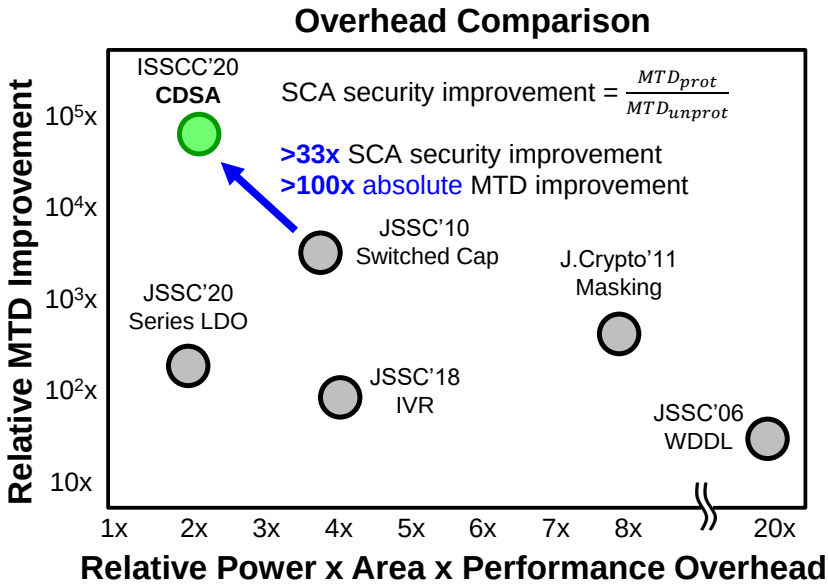


Figure 21. The CDSA-AES256 has been evaluated against both EM and power SCA attacks (CPA/CEMA) in both time and frequency domains. [22]. When subjected to CPA/CEMA attacks, the unprotected AES-256 could be broken with $\sim 10K$ traces, while the secret key for the CDSA-AES could not be revealed, even after $1B$ encryptions, showing an $100\times$ MTD improvement over the previous countermeasures with comparable overheads.

Now, for the future works, from an attack perspective, it would be interesting to analyze the effectiveness of cross-device attacks with low-SNR EM traces. Additionally, combining it with an end-to-end EM SCA attack framework such as *SCNIFFER* would reduce the attack time drastically.

Regarding the countermeasures, future works can investigate fully-digital implementations of the proposed CDSA hardware. This flexibility of such a synthesizable countermeasure would allow the industry to adopt this circuit without having to put in extra manual effort that comes with technology scaling. Additionally, to reduce the power overheads, it will be interesting to sense a power or an EM attack pro-actively and engage the countermeasure only after an imminent attack is detected.

Author Contributions: Conceptualization, D.D. and S.S.; methodology, D.D. and S.S.; software/simulations, D.D.; validation, D.D.; measurements, D.D.; writing—original draft preparation, D.D.; writing—review and editing, D.D. and S.S.; visualization, D.D. and S.S.; supervision, S.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by NSF under grants CNS 17-19235, CNS 19-35573 and in part by Intel Corporation.

Acknowledgments: The authors would like to acknowledge Josef Danial, graduate student (MS), and Mayukh Nath, PhD student, at the SPARC Lab, Purdue University, for their technical contributions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. McKinsey Global Institute. *The Internet of Things: Mapping the Value Beyond the Hype*; Technical Report; McKinsey Global Institute: New York, NY, USA, 2015.
2. O'Flynn, C.; Dewar, A. On-Device Power Analysis Across Hardware Security Domains. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, 126–153. [CrossRef]

3. Schellenberg, F.; Gnad, D.R.; Moradi, A.; Tahoori, M.B. Remote Inter-Chip Power Analysis Side-Channel Attacks at Board-Level. In Proceedings of the 2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Diego, CA, USA, 5–8 November 2018; pp. 1–7, [CrossRef]
4. Zhao, M.; Suh, G.E. FPGA-Based Remote Power Side-Channel Attacks. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–23 May 2018; pp. 229–244, [CrossRef]
5. Camurati, G.; Poeplau, S.; Muench, M.; Hayes, T.; Francillon, A. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; Association for Computing Machinery: Toronto, ON, Canada, 2018; pp. 163–177, [CrossRef]
6. Ronen, E.; Shamir, A.; Weingarten, A.O.; O'Flynn, C. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–24 May 2017; pp. 195–212, [CrossRef]
7. Krebs, B. Hacked Cameras, DVRs Powered Today's Massive Internet Outage, 2016. Available online: krebsonsecurity.com (accessed on 30 September 2020).
8. Kocher, P.; Jaffe, J.; Jun, B. Differential Power Analysis. In *Advances in Cryptology — CRYPTO' 99*; Wiener, M., Ed.; Number 1666 in Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1999; pp. 388–397, [CrossRef]
9. Quisquater, J.J.; Samyde, D. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In *Smart Card Programming and Security*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2001; pp. 200–210, [CrossRef]
10. Ramsay, C.; Lohuis, J. TEMPEST Attacks against AES. 2017. Available online: https://hardwear.io/document/slides-craig-ramsay.pdf (accessed on 30 September 2020).
11. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems—CHES 2004*; Joye, M., Quisquater, J.J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–29.
12. Chari, S.; Rao, J.R.; Rohatgi, P. Template Attacks. In *Cryptographic Hardware and Embedded Systems—CHES 2002*; Kaliski, B.S., Koç, Ç.K., Paar, C., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; pp. 13–28.
13. Hospodar, G.; Gierlichs, B.; De Mulder, E.; Verbauwhede, I.; Vandewalle, J. Machine learning in side-channel analysis: A first study. *J. Cryptogr. Eng.* **2011**, *1*, 293, [CrossRef]
14. Lerman, L.; Bontempi, G.; Markowitch, O. A machine learning approach against a masked AES. *J. Cryptogr. Eng.* **2015**, *5*, 123–139, [CrossRef]
15. Maghrebi, H.; Portigliatti, T.; Prouff, E. Breaking Cryptographic Implementations Using Deep Learning Techniques. In *Security, Privacy, and Applied Cryptography Engineering*; Carlet, C., Hasan, M., Saraswat, V., Eds.; Springer: Cham, Switzerland, 2016; Volume 10076.
16. Cagli, E.; Dumas, C.; Prouff, E. Convolutional Neural Networks with Data Augmentation against Jitter-Based Countermeasures—Profiling Attacks without Pre-Processing. In *Cryptographic Hardware and Embedded Systems (CHES 2017)*; Fischer, W., Homma, N., Eds.; Springer: Cham, Switzerland, 2017; Volume 10529.
17. Das, D.; Golder, A.; Danial, J.; Ghosh, S.; Raychowdhury, A.; Sen, S. X-DeepSCA: Cross-Device Deep Learning Side Channel Attack. In Proceedings of the 2019 56th ACM/IEEE Design Automation Conference (DAC), Las Vegas, NV, USA, 2–6 June 2019; pp. 1–6.
18. Das, D.; Maity, S.; Nasir, S.B.; Ghosh, S.; Raychowdhury, A.; Sen, S. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In Proceedings of the 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Mclean, VA, USA, 1–5 May 2017; pp. 62–67, [CrossRef]
19. Das, D.; Maity, S.; Nasir, S.B.; Ghosh, S.; Raychowdhury, A.; Sen, S. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE Trans. Circuits Syst. Regul. Pap.* **2018**, *65*, 3300–3311. [CrossRef]
20. Das, D.; Nath, M.; Chatterjee, B.; Ghosh, S.; Sen, S. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In Proceedings of the 2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 5–10 May 2019; pp. 11–20. [CrossRef]

21. Das, D.; Nath, M.; Ghosh, S.; Sen, S. Killing EM Side-Channel Leakage at its Source. In Proceedings of the 2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, 9–12 August 2020; pp. 1108–1111. [CrossRef]
22. Das, D.; Danial, J.; Golder, A.; Modak, N.; Maity, S.; Chatterjee, B.; Seo, D.; Chang, M.; Varna, A.; Krishnamurthy, H.; et al. 27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation. In Proceedings of the 2020 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 16–20 February 2020; pp. 424–426, [CrossRef]
23. Hwang, D.D.; Tiri, K.; Hodjat, A.; Lai, B.C.; Yang, S.; Schaumont, P.; Verbauwhede, I. AES-Based Security Coprocessor IC in 0.18um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks. *IEEE J. Solid-State Circ.* **2006**, *41*, 781–792. [CrossRef]
24. Sen, S.; Raychowdhury, A. Electromagnetic and Machine Learning Side-Channel Attacks and Low-Overhead Generic Countermeasures. 2019. Available online: https://ches.iacr.org/2019/src/tutorials/ches2019tutorial_Sen.pdf (accessed on 30 September 2020).
25. Akkar, M.L.; Bevan, R.; Dischamp, P.; Moyart, D. *Power Analysis, What Is Now Possible... Advances in Cryptology— ASIACRYPT 2000*; Okamoto, T., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2000; pp. 489–502. [CrossRef]
26. Poschmann, A.; Moradi, A.; Khoo, K.; Lim, C.W.; Wang, H.; Ling, S. Side-Channel Resistant Crypto for Less than 2300 GE. *J. Cryptol.* **2011**, *24*, 322–345. [CrossRef]
27. Tokunaga, C.; Blaauw, D. Securing Encryption Systems With a Switched Capacitor Current Equalizer. *IEEE J. Solid-State Circuits* **2010**, *45*, 23–31. [CrossRef]
28. Kar, M.; Singh, A.; Mathew, S.K.; Rajan, A.; De, V.; Mukhopadhyay, S. Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator. *IEEE J. Solid-State Circuits* **2018**, *53*, 2399–2414. [CrossRef]
29. Singh, A.; Kar, M.; Chekuri, V.C.K.; Mathew, S.K.; Rajan, A.; De, V.; Mukhopadhyay, S. Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO. *IEEE J. Solid-State Circuits* **2020**, *55*, 478–493. [CrossRef]
30. Golder, A.; Das, D.; Danial, J.; Ghosh, S.; Sen, S.; Raychowdhury, A. Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2019**, *27*, 2720–2733. [CrossRef]
31. Dataset/Framework. 2020. Available online: Https://github.com/SparcLab/X-DeepSCA (accessed on 30 September 2020).
32. Danial, J.; Das, D.; Ghosh, S.; Raychowdhury, A.; Sen, S. SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing. *IEEE Access* **2020**, *8*, 173414–173427. [CrossRef]
33. SCNIFFER Demo. 2019. Available online: Https://www.youtube.com/watch?v=5aVkcgyDJdE (accessed on 30 September 2020).
34. Das, D.; Danial, J.; Golder, A.; Modak, N.; Maity, S.; Chatterjee, B.; Seo, D.; Chang, M.; Varna, A.; Krishnamurthy, H.; et al. EM and Power SCA-resilient AES-256 through >350× Current Domain Signature Attenuation & Local Lower Metal Routing. *J. Solid State Circuits* **2020**. [CrossRef]
35. Das, D.; Danial, J.; Golder, A.; Ghosh, S.; Wdhury, A.R.; Sen, S. Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS. In Proceedings of the 2020 IEEE Custom Integrated Circuits Conference (CICC), Boston, MA, USA, 22–25 March 2020; pp. 1–4. [CrossRef]
36. ISSCC 2020 Demo: Hardware for Efficient Side-Channel Security. 2020. Available online: https://www.youtube.com/watch?v=sh5_SWM7o_U (accessed on 30 September 2020).