

Received September 5, 2020, accepted September 11, 2020, date of publication September 21, 2020, date of current version October 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3025022

SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing

JOSEF DANIAL¹, (Student Member, IEEE), DEBAYAN DAS¹, (Member, IEEE), SANTOSH GHOSH², (Member, IEEE), ARIJIT RAYCHOWDHURY³, (Senior Member, IEEE), AND SHREYAS SEN¹, (Senior Member, IEEE)

¹School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47906, USA

²Intel Corporation, Hillsboro, OR 97124, USA

³School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA

Corresponding author: Josef Danial (jdanial@purdue.edu)

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

ABSTRACT Electromagnetic (EM) side-channel analysis (SCA) is a prominent tool to break mathematically-secure cryptographic engines, especially on resource-constrained devices. Presently, to perform EM SCA on an embedded device, the entire chip is manually scanned and the MTD (Minimum Traces to Disclosure) 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 attack has been missing. This work proposes SCNIFFER: a low-cost, automated EM Side Channel leakage SNIFFing platform to perform efficient end-to-end Side-Channel attacks. 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 perform Correlational EM Analysis (CEMA) at that point. 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. We demonstrate SCNIFFER using a low-cost custom-built 3-D scanner with an H-field probe ($<\$500$) compared to $>\$50,000$ commercial EM scanners, and a variety of microcontrollers as the devices under attack. The SCNIFFER framework is evaluated for several cryptographic algorithms (AES-128, DES, RSA) running on both an 8-bit Atmega microcontroller and a 32-bit ARM microcontroller to find a point of high leakage and then perform a CEMA at that point.

INDEX TERMS End-to-end EM SCA attack, low-cost EM scanning, automated framework, SCNIFFER.

I. INTRODUCTION

As the internet of things (IoT) continues to grow, security of many edge nodes has become critical. With many of these edge nodes being simple microcontrollers, side-channel attacks pose a powerful threat to their security. In the world of cryptography, side-channel attacks have long been identified as a threat to the security of computing and communication systems attempting to provide confidentiality and integrity of sensitive data, since the introduction of Differential Power Analysis in [1]. By analyzing physical side-channel information, such as power consumption, timing, or electromagnetic emissions, cryptographic algorithms that are mathematically secure can be broken efficiently.

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Aljawarneh¹.

EM side-channel analysis (SCA) is a method of using the information found in the electromagnetic emissions of a cryptographic system to extract the secret key, compromising the security of such a system. Such attacks have been shown to be capable of actually extracting secret key information, as in [2] and [3]. These EM emissions originate from current consumption of an IC running cryptographic algorithms, which while flowing through the metal layers of an IC cause EM radiation as described in [4]. The EM emissions can either be caused by key-dependent operations or other operations. EM emissions caused by key-dependent operations contribute to the side-channel signal, while EM emissions caused by other operations contribute to algorithmic noise. EM SCA attacks have successfully been used in the real world on PCs, shown in [5] and [6], and also on Smart Cards, in [7], [8]. One powerful and commonly used side-channel

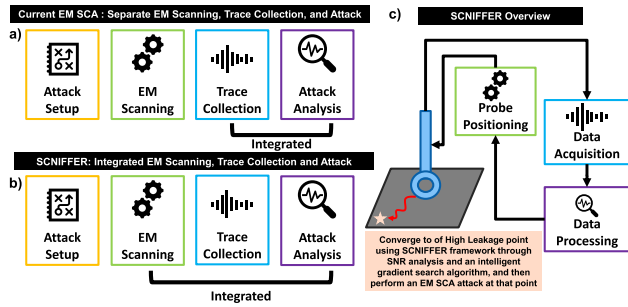


FIGURE 1. (a, b) Comparison between existing EM SCA systems and SCNIFFER. While current frameworks have integrated trace collection and attack and analysis, SCNIFFER integrates EM scanning as well. (c) High level overview of proposed SCNIFFER framework. SCNIFFER analyzes EM leakage and uses a gradient descent algorithm to locate points of high informative leakage at which the EM SCA attack should be performed.

analysis technique is correlational electromagnetic analysis (CEMA). In CEMA, EM measurements are taken while a cryptographic algorithm is executing on the target system (each measurement is known as a trace), and these traces are correlated with a leakage model, such as the Hamming Weight or Hamming Distance of data at a particular point in an algorithm [1], under a hypothesis of a subset of the secret key. In a successful attack, the hypothesis that results in maximum correlation corresponds to the secret key. Thanks to the divide and conquer nature of side-channel analysis, the cost of performing an SCA attack is linear in the key size, rather than exponential, as in brute force or other cryptanalysis methods.

A. MOTIVATION

EM side-channel attacks, while powerful in that they are non-invasive and do not require any physical changes to the system being attacked, and benefit from allowing an attacker to choose the location with maximum information leakage (SNR), introduce a number of additional challenges compared to the power SCA attacks. Firstly, as the EM signals go through a power to EM transformation that reduces amplitude compared to the measurement noise floor, meaning more traces, or more expensive measurement equipment may be needed to perform an attack. Secondly, unlike power attacks, EM attacks require attackers to choose the location of the attack in the system to capture the EM traces. However, scanning a device to determine this point is not currently integrated into current frameworks (Figure 1(a)). This choice of location can have a drastic impact on the effectiveness and efficiency of an attack. As seen in Figure 2, depending on where the EM probe is placed on a chip, the MTD for a CEMA attack can vary by $>20\times$, even for the small 9mm x 9mm Atmega and STM microcontrollers used as the target devices for this work. Current methods for determining the best location to perform CEMA are based on exhaustive search, simply performing a CEMA attack at most locations. Alternatively, it is also possible to choose an arbitrary location, and use as many traces as necessary to perform the CEMA. Practically, if the size of the system is larger, finding

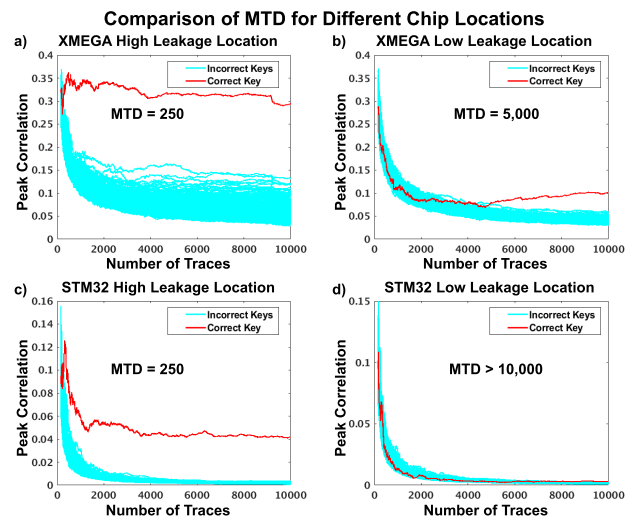


FIGURE 2. The difference in MTD between a CEMA attack at a point of high leakage vs. at a point of low leakage for both an 8-bit XMEGA microcontroller (a, b) and a 32-bit STM32F3 microcontroller (c, d). At a location of high leakage, the correct key separates in 250 traces for both microcontrollers, while a low leakage location requires $>20\times$ more traces on the XMEGA. At a low leakage location on the STM32F3, the key does not separate at all within 10,000 traces.

the correct location of the EM leakage becomes extremely challenging and requires scanning the entire chip/system.

Given the limitations of present attack systems, in this work, we propose a low-cost, fully automated, end-to-end platform for performing efficient EM side-channel attacks. SCNIFFER integrates EM scanning, trace collection, and attack/analysis into a single framework (Figure 1(b)). A high level overview of the SCNIFFER framework is shown in Figure 1(c). The core of this framework is a $\sim\$200$ 3-D printer, which we have modified to utilize as a low-cost EM scanner. SCNIFFER also uses a greedy gradient-search heuristic using a leakage measure, such as test vector leakage assessment (TVLA), or SNR to quickly and automatically locate a point of high data-dependant leakage (referred to as simply high leakage throughout this work). Finally, once the point is determined, the proposed SCNIFFER framework performs the correlational or differential EM analysis (CEMA/DEMA) at this point. While both CEMA and DEMA are possible attacks, throughout this work, we will demonstrate results with CEMA. Such an automated low-cost attack platform significantly increases the threat surface for IoT devices, however, it should be noted that SCNIFFER does not constitute a new attack; and existing countermeasures against EM SCA attack are effective against SCNIFFER.

B. CONTRIBUTION

Specific contributions of this article are:

- **Low-cost Automated EM Side-channel Analysis Framework:** A fully-automated system for efficiently scanning a cryptographic chip and finding a location of high leakage to mount an end-to-end EM SCA attack is proposed. The entire attack set-up is extremely

low-cost, owing to the custom-built EM scanner (adapting a ~\$200 3-D printer) used for mounting the attack, compared to the commercially available EM probe stations, which are very costly (>\$50,000). The system achieves 100 μ m spatial resolution, and has a scan range of 220mm \times 220mm, and is easily replicable (Section 3).

- **Integrated EM Scanning, Trace Collection, and Attack:** EM Scanning is brought in the loop of the attack framework through the proposed greedy gradient-descent heuristic algorithm, which analyzes leakage on-the-fly to efficiently scan the chip and locate a point of high leakage. This algorithm converges to a high leakage location on an $N \times N$ chip within $O(N)$ iterations. This algorithm is evaluated with both TVLA and SNR as the measures of leakage, and results for the complete system on a variety of cryptographic targets are shown (Sections 4, 5, 6).

C. PAPER ORGANIZATION

The remainder of the paper is organized as follows. Section 2 provides the background and summarizes the existing works on EM Scanning and side-channel attacks. In Section 3, the SCNIFFER framework is introduced and the low cost, custom-built EM scanning platform is presented. Section 4 describes two options for measuring leakage, TVLA and SNR, and provides motivation for finding a point of high leakage. In Section 5, the gradient-descent algorithm for efficiently determining a point of high information leakage is proposed. Next, Section 6 provides results of running the system on microcontrollers of varying architectures, cryptographic algorithms executed, and measures of leakage. Finally, Section 7 concludes the paper.

II. BACKGROUND AND RELATED WORK

IoT devices have been successfully attacked using side channel attacks, for example CPA was used to extract encryption keys from Philips Hue smart lamps in [9]. EM side-channel attacks were first proposed in [10], and share many properties with power side-channel attacks, however, can be performed at a distance, even up to one meter, as in [11]. One of the most powerful EM SCA attacks is CEMA, which is the straightforward application of Correlation Power analysis (CPA) [12] on EM traces.

However, to make these profiled and non-profiled EM SCA attacks more practical and real-time on any embedded platform/device, the trace capture and the attack needs to be automated and more efficient.

SCNIFFER can use several methods of assessing leakage, for instance, simple signal magnitude, Test Vector Leakage Assessment (TVLA) [13], or SNR [14]. In **TVLA**, two sets of traces are collected. In one set, both the key and plaintext used as input to the algorithm under test are kept fixed, and in the other the plaintext is varied randomly, while the key remains fixed. To assess the leakage, one then performs Welch's t-test for each time point of the trace. Welch's t-test is given by

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{\frac{s_1^2}{N_1} + \frac{s_2^2}{N_2}}}, \text{ where } \bar{X}_1, \bar{X}_2 \text{ are the sample means of the two}$$

sets, s_1, s_2 are sample standard deviations for the sets, and N_1, N_2 are the sizes of the sets. If the maximum t-value at a point is above 4.5, one can conclude leakage is present with 99.999% confidence. Meanwhile, we consider the signal to noise ratio as defined in [14], to be $SNR = \frac{VAR[Q]}{VAR[N]}$, where Q is the side channel leakage, and N is the noise. Unlike TVLA, which does not guarantee exploitable leakage, SNR defined in this way can be directly related to the success rate of a CEMA attack [14].

Once SCNIFFER has chosen a point to attack, CEMA is used to recover the secret key. CEMA revolves around making hypotheses on secret values, then predicting the EM leakage of an intermediate variable based on the key. Measurements (traces) are taken while the device performs encryption, then the measurements are correlated with the predicted leakage for all hypotheses. The hypothesis that results in the largest correlation is taken as the guess for the secret value. The number of traces needed to recover the key in this way is then the minimum traces to disclosure (MTD). In this work, the secret values are the bytes of the AES key, and the intermediate variable is the first round sbox output, and Hamming Weight, that is, the number of 1's in the binary representation of this variable, is used as the leakage model of data at this point.

Addressing the issue of finding where a chip leaks the most EM radiation has been investigated in [15], and [16]. EM scanning with a focus on side-channel attacks, that is, determining where the most cryptographic information leaks within a chip has been addressed in [17], [18], and [19]. However, such methods focus on observing the leakage over the entire chip, not efficiently finding the point or region of the maximum leakage. This causes these methods to take a long time and a majority of the time is spent collecting data that is unnecessary for an attacker. Even in recent years, exhaustive search is used in many EM attacks, including an attack against threshold implementations in [20] which uses multiple EM probes simultaneously, and against leakage-resilient pseudo-random functions in [21]. These attacks use localized EM leakage to perform attacks more efficiently than with power, but rely on exhaustive search to find localize the leakage. More recently in [22], an adaptive method to determine the location of greatest cryptographic leakage without resorting to exhaustive search is presented. However, this method performs a full SCA attack at each location analyzed, again making it unsuitable for an attacker, whose goal is only a single successful attack. By creating a framework that minimizes this unnecessary data collection, EM side-channel attacks can be made more efficient, powerful, and practical, requiring far fewer traces to reveal the secret key of the cryptographic algorithm. Additionally, these platforms can be orders of magnitude more costly than the system proposed in this work, for instance the Riscure EM Probe station [23] itself can cost ~\$50,000, while the entire SCNIFFER system costs <\$500. Table 1 compares the SCNIFFER system to

TABLE 1. Comparison with previous works. SCNIFFER is significantly lower cost compared to previous works, and additionally is the only system designed to maximize the effectiveness of an attack, as other systems seek only the location of most informative leakage.

	Search Technique	Search Metric	Attack Technique	Positioning Accuracy	Cost	System Focus
[18]	Exhaustive Search	SNR	CEMA	100 μ m	>\$10,000*	Leakage Localization
[19]	Exhaustive Search	Difference of Means	Template Attack	50 μ m	>\$10,000*	Leakage Localization
[20]	Exhaustive Search	Correlation	Template Attack	167 μ m	>\$50,000*	Threshold Attack
[21]	Exhaustive Search	SNR	Template Attack	70 μ m	>\$10,000*	PRF Attack
[22]	Greedy Search	DEMA	DEMA	2.5 μ m	>\$50,000*	Leakage Localization
This work	Gradient Search	TVLA/SNR	CEMA	100 μ m	~\$500	End-to-End Attack





* Estimated cost of system based on listed components and specifications

previous works. Note that while all previous works as shown in the table aim to locate the point of greatest informative leakage, only SCNIFFER focuses on minimizing the total number of traces needed for a successful attack. SCNIFFER is the first fully-automated, efficient EM SCA attack framework and the system is described in the following section.

III. SCNIFFER: LOW COST AUTOMATED EM SCANNING

The SCNIFFER system is designed for low cost and automation. In this section, we first describe the physical components that make up SCNIFFER, then discuss the automation aspect of the system.

TABLE 2. Summary of the main components of the SCNIFFER system, their costs, performance, and a comparison to Riscure's EM Probe station.

	Scope	Scanner	Amplifier	Probe
Picture				
Cost	\$250	\$200	\$130	\$50
SCNIFFER Specifications	10-bit ADC 105 MS/s	100 μ m	20dB	16mm ²
Model	Chipwhisperer-Lite	Ender 3	Tekbox TWBA2	Tekbox TBPS01
Riscure EM Probe Station Specifications	-	2.5 μ m	-	1mm ²

A. LOW COST EM SCANNING SETUP

The scanning hardware consists of an Ender-3 3-D printer [24] with a 10mm loop diameter H-field probe attached to the extruder, the Chipwhisperer [25] platform for interfacing with the victim (The CW309T-XMEGA mounted on the 308 UFO Target board) and trace collection, an amplifier to amplify the EM probe output, and finally a PC to control both the 3-D printer and the Chipwhisperer Lite capture board. While such EM scanning systems do exist, for instance, Riscure's EM Scanning Station, we chose to create such a system from scratch for the following reasons: 1) Commercial scanning systems (like Riscure [23]) scanning station is orders of magnitude more expensive and 2) It is very straightforward to interface with the custom system to develop the scanning algorithm. As seen in Table 2, the cost

of a commercial scanner is orders of magnitude higher than SCNIFFER, and while it is hard to know if this price has been inflated by the selling company, it is reasonable for prices to be higher, as there are not many EM scanners on the market.

To manipulate the probe, an Ender-3 3-D printer, running stock firmware was used. This model of printer has a minimum step size of 0.1mm, and can be controlled via a USB serial connection. It has a maximum movement speed of 180 mm/s, with a print area of 220mm \times 220mm \times 250mm. The precision and speed offered by this 3-D printer are sufficient to complete a 50 \times 50 scan of the 9mm \times 9mm IC used in testing in an acceptable time. Additional justification for the choice of printer, beyond the cost includes the ease of interfacing, the form factor, maintainability, and software support. The open source firmware used by this printer is well documented, and can be controlled through an exposed serial port, making interfacing very easy. The printer also has an open form factor that allows the probe and victim board to be mounted easily. While the durability and hardware support would not be as good as a commercial EM scanner, the simple construction and use of off-the-shelf components make maintenance straightforward. The software support is quite strong, being open source, and the printer is plug-and-play compatible with any device with a serial port. The system is capable of performing a 30 \times 30 scan of the chip in \sim 15 minutes, and perform an amplitude scan in \sim 75 minutes. The probe used is a commercial H-field probe for performing EMC measurements, and the signal is amplified before being passed to the Chipwhisperer capture board. *While the probe used does not have extremely high spatial resolution, the probe resolution matches the scan resolution*, allowing heatmaps such as the one in Figure 4(a) to be created, and Chipwhisperer is able to capture enough information leakage for the target devices considered, leading to low MTDs when probed at appropriate locations, as seen in Figure 2, while still being low cost. Even though this probe is on the larger side, the SCNIFFER platform is compatible with more sensitive probes and is expected to become more precise with such probes. The complete system is shown in Figure 3(a) showing the 3-D printer, the probe, Chipwhisperer system, and PC. The probe and victim IC are shown in detail in Figure 3(b). The probe position can be controlled manually, through the 3-D printer controls, or programmatically through the serial connection to a PC, as it is in the SCNIFFER system.

The major cost savings in the SCNIFFER system come from using a low cost 3-D printer to control the probe, instead of a high cost motorized table. The total cost of the 3-D printer, probe and amplifier used in SCNIFFER is \sim \$500, which is a few orders of magnitude less expensive than many motorized tables by themselves, and nearly two orders of magnitude less expensive than systems such as Riscure's EM probe station (\sim \$50,000). While more expensive scanners, probes and measurement systems could improve spatial and frequency resolution, such a system would only be available to very sophisticated attackers. As SCNIFFER aims to demonstrate that practical, low-cost attacks are possible

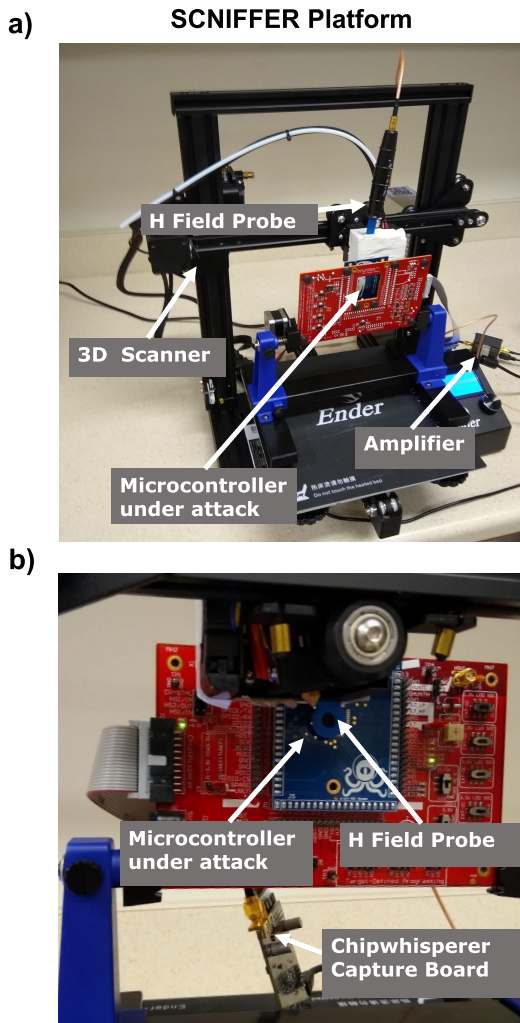


FIGURE 3. (a) The complete EM Scanning and trace capture set-up system, including the 3-D printer, Chipwhisperer system, EM probe, amplifier, and victim. (b) Close-up of scanner, showing probe and victim board.

using systems two orders of magnitude cheaper than existing scanners, high-cost, high resolution components are not used. Table 2 summarizes these components, including their costs and performance compared to the Riscure system.

B. AUTOMATED EM SCANNING

Now that the SCNIFFER system's low cost hardware has been described, we move to the automated scanning and attack procedure. The basic premise of the automated system is to locate a point on the target device where the chosen leakage measure is high by using the scanning algorithm specified in Section 5, and then to automatically perform CEMA at this point. This removes the need for an expert to manually analyze example traces to choose a location for an attack.

During an attack, the probe is positioned at a location dictated by the intelligent scanning algorithm, then, the appropriate ADC phase for trace collection is determined by capturing

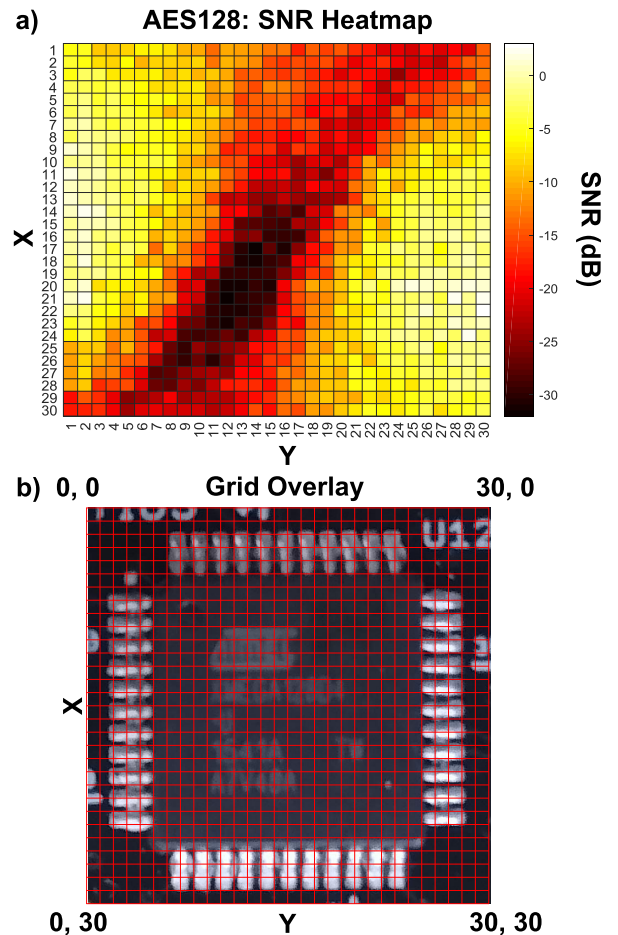


FIGURE 4. (a) Heatmap of the SNR values obtained by performing a full 30×30 scan of the 8-bit target microcontroller. (b) This shows the grid divisions where leakage measurements were performed. 1000 traces were used to compute the SNR values at each point. The part of the target microcontroller board which leak the most information can be observed.

traces at varying ADC phases, and the phase giving the largest average amplitude is chosen for further measurements at that particular point. The signal is sampled at 29.48MHz, $4 \times$ the clock frequency of 7.37MHz, so clock edges are aligned to samples. The signal is amplified by the external amplifier, as well as the Chipwhisperer internal amplifier (set to a gain of 34.5dB), but no other preprocessing is performed. Chipwhisperer is then used to capture traces for leakage measurement (through SNR, TVLA or other measures) and finally CEMA is performed at the location found by the algorithm to have the highest leakage. Example leakage measures tested with SCNIFFER, and the development of the intelligent scanning algorithm, along with detailed results are described in the following sections.

IV. SIGNAL LEAKAGE MEASUREMENT USING SCNIFFER

As the choice of probe location is a major factor in determining the number of traces needed to recover a key in CEMA as shown in Figure 2, this location must be chosen intelligently.

Currently, this is done by either exhaustive search of the entire chip, or by an expert evaluating sample EM traces at several locations, and choosing a location based on visual inspection of the traces. While an exhaustive search will certainly produce the best location to attack, it requires a large amount of time, especially for systems with a large initial MTD. Choosing a location based on visual inspection of traces may result in a location that can be attacked, however not necessarily the best in terms of MTD. Additionally, this method requires an expert to perform the inspection of traces. In this work, we aim to fully automate the process of choosing a location as an expert might, by looking at measures of leakage, and finding a location with high leakage. As with a manual choice, this location may not be the location corresponding to the lowest MTD, but should leak enough information to be attacked in a reasonable amount of time, without the need for an expert.

SCNIFFER is designed such that any measure of leakage can be used. For example signal amplitude, Test Vector Leakage Assessment (TVLA) [13], or SNR could be used, and the SCNIFFER platform will be able to converge to a location where the leakage measure is high in $O(N)$ measurements. We provide results using both TVLA and SNR, both described, and then compared in the following subsections.

A. SIGNAL AMPLITUDE FOR LEAKAGE MEASUREMENT

As motivation for why side-channel leakage measures must be used with SCNIFFER to locate low MTD locations, we measure the signal amplitude at each point of the victim chip, producing the heatmap seen in Figure 7(b). The amplitude was measured as the mean square amplitude of each trace, averaged across 10 traces. As can clearly be seen in that figure, the amplitude does not correlate to the MTD at all, as expected.

Hence, further results are shown using one of the two leakage measures explained in the following sections, TVLA and SNR. While these are the measures chosen for demonstrating SCNIFFER, they are by no means the best nor the only measures that can be used, as SCNIFFER does not rely on specific leakage type, only requires that the leakage correlate with the MTD. Determining the best measures of leakage in terms of the attack success rate and minimum number of traces required is a future research direction.

B. TVLA FOR LEAKAGE MEASUREMENT

While signal amplitude is quick to measure, it has no relationship to side channel leakage. As the goal of SCNIFFER is to locate a position with high side channel leakage, amplitude is therefore not a good measure. A measure that does consider side channel leakage, and may be a better fit for SCNIFFER is TVLA. While high t-values from TVLA may not necessarily imply a low MTD, it allows locations where leakage is detected with high confidence to be focused on. The TVLA performed is the non-specific, fixed versus random t-test. We choose $N = 200$ for the number of traces in each group, for a total of 400 traces per TVLA performed.

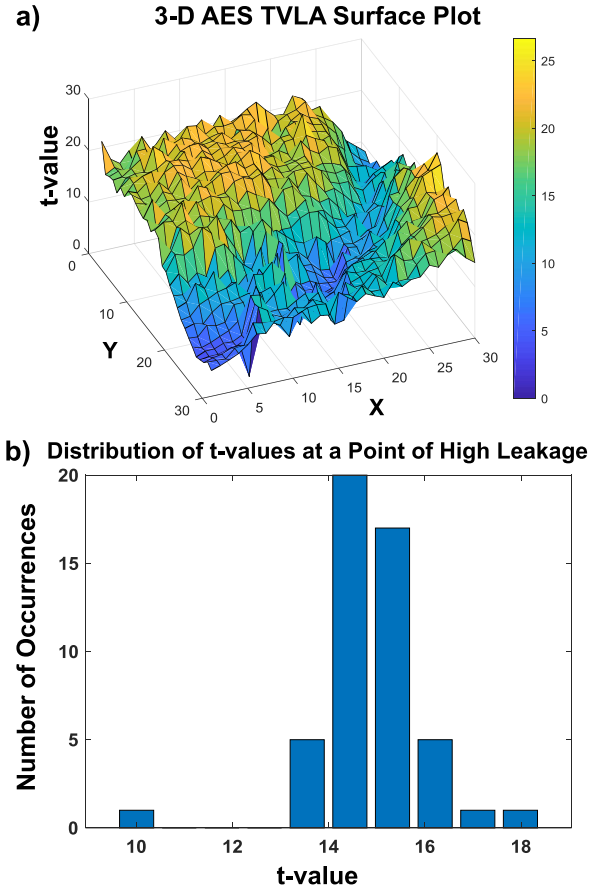


FIGURE 5. (a) TVLA surface plot. Again, the surface is not smooth or monotonic, as there are many local minima and maxima, as in Figure 6(a). (b) Histogram of TVLA measurements at a single point. 50 TVLA measurements were made at a point of high leakage, each done as in (a), using 400 traces each. Given the distribution much wider seen in (b), the increased roughness of the surface in (a) can be explained.

This number of traces creates large separation between points of low leakage and ones of high leakage, as seen in Figure 5(a), where the high leakage location reaches a t-value of 22, while the low leakage location only reaches a t-value of 4. Note that the TVLA surface is rough, with many local minima and maxima. Even at a fixed location there is variance in the TVLA measurements, shown in Figure 5(b). However, it is infeasible to perform many TVLA measurements at each point to average out this noise.

C. SNR FOR LEAKAGE MEASUREMENT

Compared to amplitude and TVLA, SNR, as defined in [14] requires more traces, however has a direct relationship to the MTD. Given this relationship, one can estimate the MTD, thus a location maximizing SNR will minimize MTD. 1000 traces were used to calculate the SNR, as for the 8-bit microcontroller used, this gave large separation between locations of high and low leakage, as seen in Figure 6, where the SNR varies from -30dB to 3dB . SNR is calculated using the same intermediate variable and leakage model as the CEMA used, that is, the first round sbox output and the the Hamming

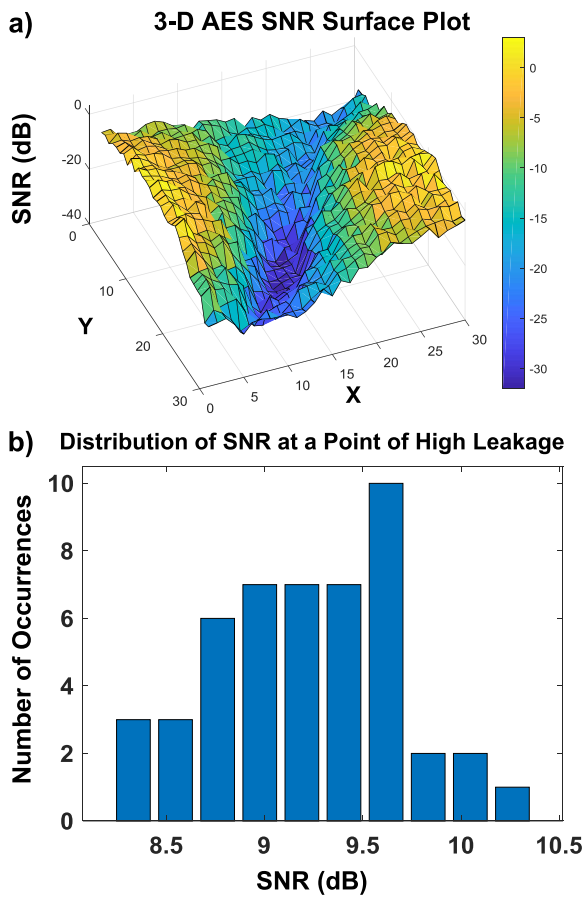


FIGURE 6. (a) SNR surface plot of the same scan as Figure 4(a). Here it can be clearly seen that the surface is not smooth or monotonic, as there are many local minima and maxima. (b) Histogram of SNR measurements at a single point. 50 SNR measurements were made at 1 point. This distribution can explain some of the roughness of the surface seen in (a).

Weight model, respectively. Like with TVLA, the surface is somewhat rough, but again it is infeasible to take many SNR measurements to average out this noise.

D. CORRELATION AMONG AMPLITUDE, TVLA, SNR, MTD

While signal amplitude, TVLA, and SNR can all be used with SCNIFFER as measures for leakage, since the end goal of the SCNIFFER system is to perform an attack, we investigate how these measures compare to the MTD at each location. To compare the measures, a 10×10 scan of the chip was carried out, and CEMA was performed using 1,000 traces at each point. The resulting heatmap, along with heatmaps for SNR, TVLA, and amplitude, are shown in Figure 7, and the methods are summarized in Table 3. From these results, clearly TVLA and SNR both appear to correlate to the MTD strongly, however amplitude correlates very poorly. While signal amplitude is easy to measure, there is no guarantee that this measure correlates to the MTD, as high signal leakage does not imply high information leakage. Additionally, an uncorrelated EM source having high signal leakage

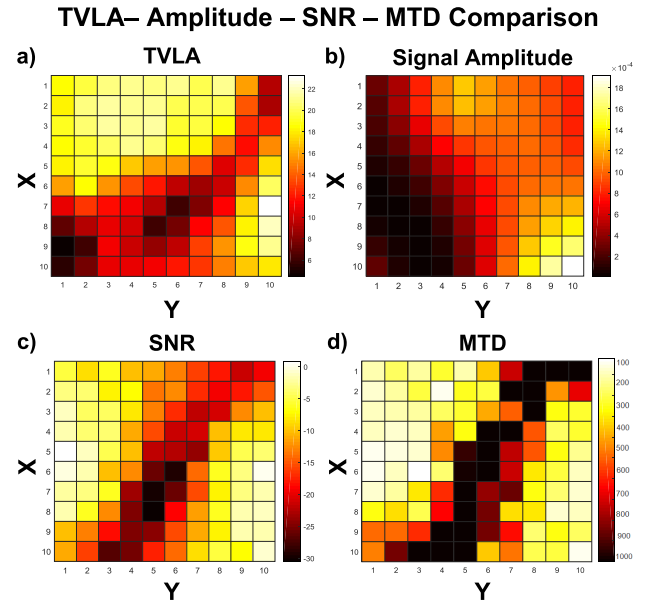


FIGURE 7. 10×10 heatmap of (a) TVLA values (b) signal amplitudes (c) SNR values and (d) MTDs. From these plots TVLA and SNR appear to correlate to MTD much better than the signal amplitude. While amplitude is easy to measure, it is clear that high amplitude of leakage does not necessarily correspond to high information leakage.

TABLE 3. Summary of investigated leakage measures, and comparison to MTD.

	Amplitude	TVLA	SNR	MTD
Traces Used	20	400	1,000	1,000
Leakage Detected	All EM Leakage	Data Dependent Leakage	Exploitable Leakage	Exploitable Leakage
Correlation to MTD	Low	High	Highest	-

could confuse an attacker into choosing a poor location to attack. While TVLA also does not guarantee high exploitable leakage, it can be used to identify and focus on regions where leakage is detected with confidence. Additionally, for the microcontroller considered in this work, TVLA does empirically correlate to the MTD quite well, even if it is not guaranteed to be the case in general. Finally, as SNR is directly related to the attack success rate, it unsurprisingly is highly correlated in practice. Further, due to this correlation, the location of highest SNR will theoretically be the location of lowest MTD, achieving SCNIFFER's goal.

V. GREEDY GRADIENT-SEARCH HEURISTIC

A critical piece of the SCNIFFER system is the algorithm for locating the point of high leakage at which the attack should be performed. It is through this algorithm that the SCNIFFER attack framework gains benefits over an exhaustive search, as the high leakage location in an $N \times N$ grid can be found with N measurements as opposed to N^2 . As an example, we use SNR as the leakage measure to demonstrate the performance of the SCNIFFER greedy gradient-search algorithm throughout this section. The remainder of

this section describes the algorithm in detail, and provides results of running the algorithm on an Atmel XMEGA 8-bit processor running software AES.

A. ALGORITHM DESCRIPTION

To avoid taking measurements at all possible points, we propose a heuristic search algorithm for finding a point of high leakage in a minimum number of scans. The search algorithm works in two phases. In the first phase, the search space is divided into an $M \times M$ grid, where M is the initial grid size parameter, and the leakage is measured at the center of each grid cell. This initial grid must be more coarse than the measurement grid, which would be $N \times N$. Then in the second phase, a gradient search algorithm is started from the point of the highest leakage found in the first phase. The gradient is computed by measuring the leakage of the four grid cells adjacent to the current cell, then treating each measurement as the magnitude of a vector whose direction is the direction from the cell where the gradient is being estimated to the cell where the measurement was made. The sum of these vectors is treated as the estimate of the gradient. The next point to measure is determined by adding a vector in the direction of the gradient with a magnitude of stepSize to the current location. This location is then mapped to a grid cell, and the leakage is next measured in the center of this resulting grid cell. Given this method, movement is restricted to be between grid cells, and is not entirely arbitrary, however movement to diagonal cells or moving multiple cells at once are possible moves, depending on the stepSize parameter.

If the algorithm attempts to measure outside the search space, it will instead move only to the edge and then stop. A maximum number of iterations can also be specified, along with an “iterations without improvement” stopping criteria. The “iterations without improvement” parameter should be set to a sizeable fraction of the grid resolution N , for values too small, several iterations may pass without improvement, especially for noisy surfaces, and the algorithm may stop prematurely. This two phase process is described in Algorithm 1.

B. ALGORITHM PERFORMANCE

Based on experimental results, the algorithm is able to locate a point of high leakage in a $N \times N$ grid of possible measurements in $\approx N$ SNR measurements. Figure 8 demonstrates that as the search grid size increases by N^2 , the number of tests required only increases by N , showing the improvement over an exhaustive search is more drastic as the size of the scan increases, either due to increased resolution or larger scan area. We also see the effect of the parameters of the algorithm, and see how varying them affects performance. In Figure 9(a), where, by increasing the resolution of the initial search grid, the lowest MTD found for a given number of measurements changes. As expected, as more initial points are scanned, fewer gradient steps are required to converge to the high leakage location. In Figure 9(b), the step size is varied, and we see that for a small step size, the algorithm gets stuck in a local minimum, and does not converge to the point of high leakage

Algorithm 1 Gradient Search Heuristic to Find the High Leakage Location

```

 $N$  = Grid Resolution;
maxLeakage = 0;
initLocs = getInitialLocations(initialGridSize,  $N$ );
for  $loc \in \text{initLocs}$  do
    moveProbe( $loc$ );
    leakage = getLeakage();
    if leakage > maxLeakage then
        maxLeakage = leakage;
        startLoc =  $loc$ ;
    end
end
moveProbe(startLoc);
bestLoc = startLoc;
 $m$  = startLoc;
while Not Converged do
    delta = getDelta(get4Neighbors());
     $m$  =  $m$  - stepSize * delta;
    moveProbe( $m$ );
    leakage = getLeakage();
    if leakage > maxLeakage then
        maxLeakage = leakage;
        bestLoc =  $loc$ ;
    end
end
end

```

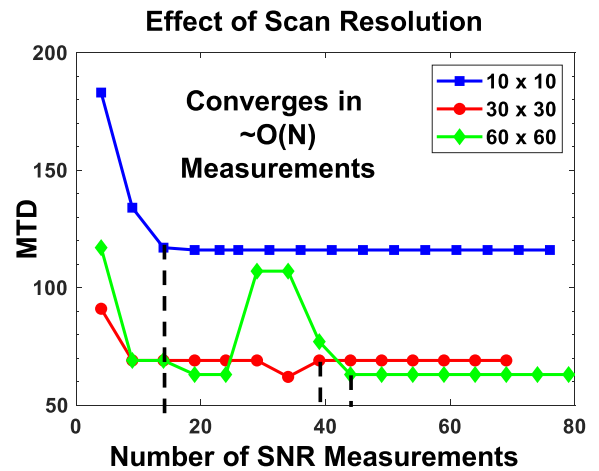


FIGURE 8. Leakage vs. number of SNR measurements for varying grid scales. Each SNR measurement is computed using 1000 traces collected at the measured location. The data for the 30×30 grid was the same as in Figures 4 and 6(a). The full 60×60 and 10×10 grids were also collected, allowing the performance of the algorithm to be seen at various degrees of measurement resolution. Through these results, it can be seen that even as the size of the search space increases by N^2 , the time to converge increases by only N .

the other step sizes do. It is worth noting that even though the algorithm gets stuck in a local minimum, the initial grid search, SCNIFFER still finds a relatively low MTD location. A larger step size also converges, and if the step size is too large however, the convergence is slower, and less smooth,

Effect of Parameters on Algorithm Performance

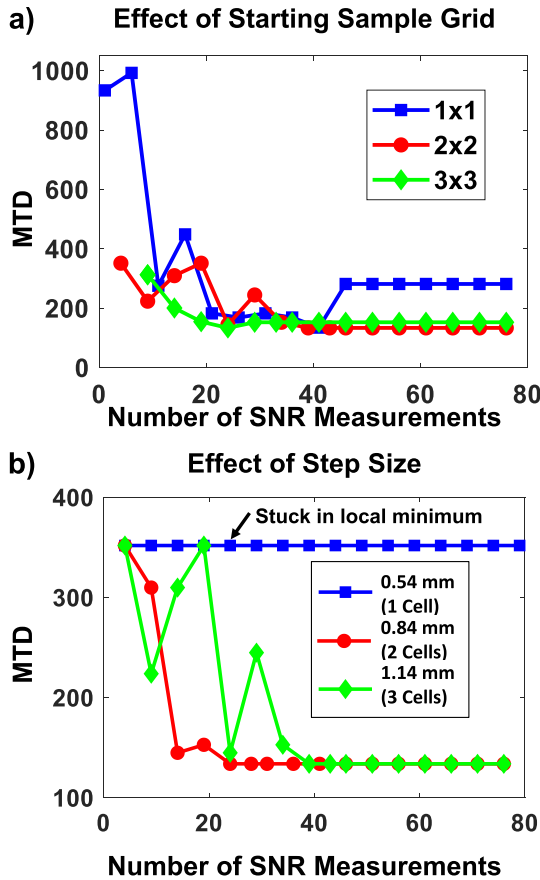


FIGURE 9. (a) MTD vs number of SNR measurements performed for varying the initial sample grid size parameter. Note that the 2×2 and 3×3 grids locate the point of high leakage within 40 SNR measurements, while a single initial sample point results in a higher MTD, and after 45 such measurements. For all initial sample grid sizes, a step size of 1.14mm was used. (b) This demonstrates the effect of step size on performance. A step size too small can result in the algorithm getting stuck in a local maximum, and in this case as the step size increased, convergence sped up, however, for much larger step sizes, it is possible to overshoot the location of highest leakage, resulting in slower, less smooth convergence. For all step sizes, a 2×2 initial sample grid was used. Both (a) and (b) used a 30×30 scan resolution.

as it may step over the best point. Note that the effective step size is a function of both the resolution of the scan, N , and the step size parameter of the algorithm. This, along with the dimensions, L , of the chip allow calculating the effective step size as $\frac{1}{N} * L \text{ mm} * \text{StepSize}$. Given these results, one can see that for reasonable choices of parameters, the algorithm is observed to converge to a point of high leakage in $O(N)$ steps for an $N \times N$ grid of measurements, providing SCNIFFER with a significant improvement over an exhaustive search.

VI. RESULTS

In this section, we provide results of using the SCNIFFER framework in various scenarios. We start with the results of an attack using TVLA, then with SNR. Following this, we provide a short discussion of the number of traces needed

in a SCNIFFER attack. We then show the performance of the TVLA and SNR based attacks for a variety of cryptographic algorithms. Next, results comparing the 8-bit architecture chip used so far to a 32-bit architecture chip are shown, again for both TVLA and SNR measures. Finally, we show results showing the effects of a masking countermeasure, using the SNR based attack.

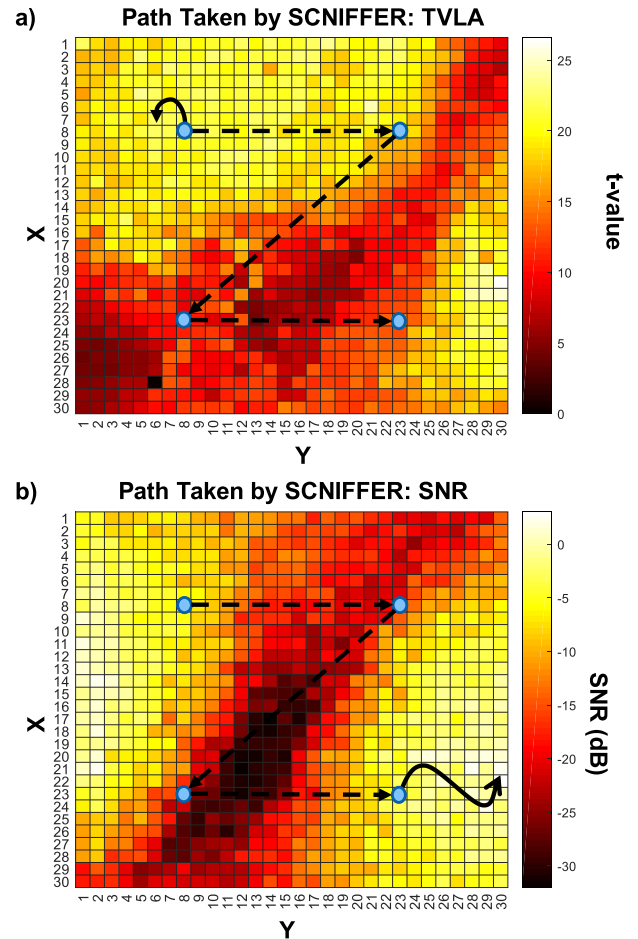


FIGURE 10. Heatmaps for AES running on the 8-bit microcontroller, with the path taken by SCNIFFER shown for TVLA in (a), and SNR in (b). The same search algorithm parameters were used in all cases.

A. TVLA BASED SCNIFFER

While it is not guaranteed to correlate with MTD, TVLA can be used with the SCNIFFER algorithm. The path taken for this case is shown in Figure 10(a). This path remains in the zone of high TVLA values, and as TVLA correlates well with MTD in our experiments, this location has a very low MTD, seen in Figure 11(b), and is among the lowest on the chip. TVLA at each location requires a total of 400 traces to compute TVLA, and additional traces would be needed for systems with lower SNR, as we describe in section IV D. Additionally, as the TVLA surface is not smooth, convergence is slightly slowed, increasing the attack time.

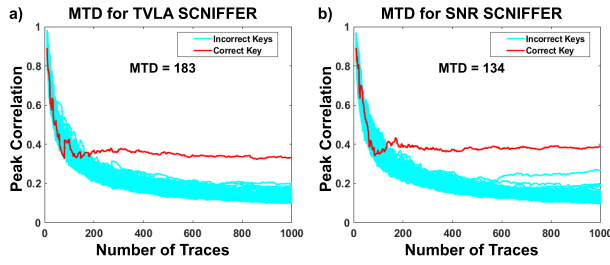


FIGURE 11. MTD plots at locations found by SCNIFFER using TVLA as a leakage measure (a), and SNR as a leakage measure (b). While the MTD is not the minimum, it is fairly close to the minimum for both measures, with SNR having a slightly lower MTD than TVLA.

TABLE 4. Comparison of different leakage measures used with SCNIFFER, as well as results of a full exhaustive search. The total traces includes the traces needed for the initial search, gradient search, and CEMA. The exhaustive search total traces includes a 1000 trace CEMA at all 100 locations.

Leakage Measure	Convergence Location	MTD	Total Traces
TVLA	(2, 2)	183	5,807
SNR	(7, 10)	134	10,134
Exhaustive	(3, 6)	91	100,000

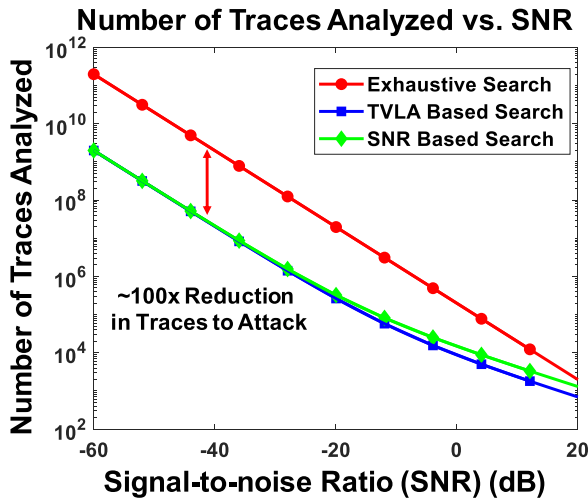


FIGURE 12. Number of traces required for TVLA and SNR based SCNIFFER compared to exhaustive search vs. SNR for the case of a 10×10 scan. The $\sim 100\times$ reduction is due to the fact that an exhaustive search must perform a CEMA at each location, while SCNIFFER only visits N locations.

B. SNR BASED SCNIFFER

In contrast to TVLA, which does not guarantee leakage found is exploitable, SNR does, as it is related to the MTD. We see that SNR based SCNIFFER does take a different path than TVLA, and converges to a different location. The MTD at this location is slightly lower than the TVLA location, but still not the absolute lowest found on the chip. Furthermore, to accurately measure SNR, more traces than TVLA are needed for measurement, increasing the number of traces needed, and this number increases as the SNR reduces, as discussed in section IV D. Despite this, once the SNR reduces below a certain point, shown in Figure 12, a SNR-based SCNIFFER

attack becomes as efficient as a TVLA-based attack, with the additional guarantee of exploitable leakage.

C. NUMBER OF TRACES NEEDED FOR SCNIFFER ATTACKS

The performance of the SCNIFFER platform can be quantified and compared to other methods by investigating how the total number of traces needed to perform an attack changes as the SNR of the device under attack changes. Previous works have shown in [26] and [14] that the MTD for a CEMA attack is related to the SNR of the signal used in the attack by $MTD = k_0 * \frac{1}{SNR}$. Additionally, [27], [28] have shown that the number of traces needed to perform a TVLA (N_{TVLA}) or calculate SNR (N_{SNR}) is also related to SNR by $N_{TVLA} = c_0 * \frac{1}{SNR}$ and $N_{SNR} = c_1 * \frac{1}{SNR}$. From there, it is straightforward to quantify the performance of an exhaustive search and SCNIFFER using both TVLA and SNR as follows,

$$N_{SCN-TVLA} = N * c_0 * \frac{1}{SNR} + k_1 * \frac{1}{SNR^2} \quad (1)$$

$$N_{SCN-SNR} = N * c_1 * \frac{1}{SNR} + k_1 * \frac{1}{SNR^2} \quad (2)$$

$$N_{exh} = N^2 * k_1 * \frac{1}{SNR^2} \quad (3)$$

where $N \times N$ is the resolution of the grid scan, and k_0, k_1 , and c_0 are arbitrary constants chosen such that the models match the results presented.

A SCNIFFER attack requires measurements to be made at approximately N points for an $N \times N$ grid, as the search algorithm requires $O(N)$ measurements, with each requiring N_{TVLA} in the TVLA case and N_{SNR} in the SNR case. Additionally a single CEMA attack requiring MTD traces is needed, resulting in equations (1) and (2). An exhaustive search on the other hand would require a CEMA to be performed at all N^2 locations, resulting in equation (3). These trends are pictured in Figure 12, which clearly shows the $100\times$ reduction in required traces in the case of a 10×10 scan for low values of SNR. This reduction can be explained by the fact that the number of traces needed to measure TVLA or SNR changes as $\frac{1}{SNR}$, compared to the MTD which changes as $\frac{1}{SNR^2}$. Additionally, the number of points traversed is only N , as opposed to N^2 for an exhaustive search. Also, we see TVLA slightly outperforms SNR in terms of number of traces needed to perform an attack when SNR is high. For low SNR, the performance of both measures is mostly equivalent, as the number of traces needed is dominated by the CEMA, and using SNR as the leakage measure gives guarantees on the success rate of the CEMA, which TVLA does not.

D. EFFECT OF CRYPTOGRAPHIC ALGORITHM ON CONVERGENCE

Next, in Figure 13(a), the effect of different cryptographic algorithms running on the target microcontroller can be seen, when using TVLA. For AES, DES, and RSA, the gradient search algorithm converges a point of high leakage in a similar number of traces. A 30×30 scan was performed for all

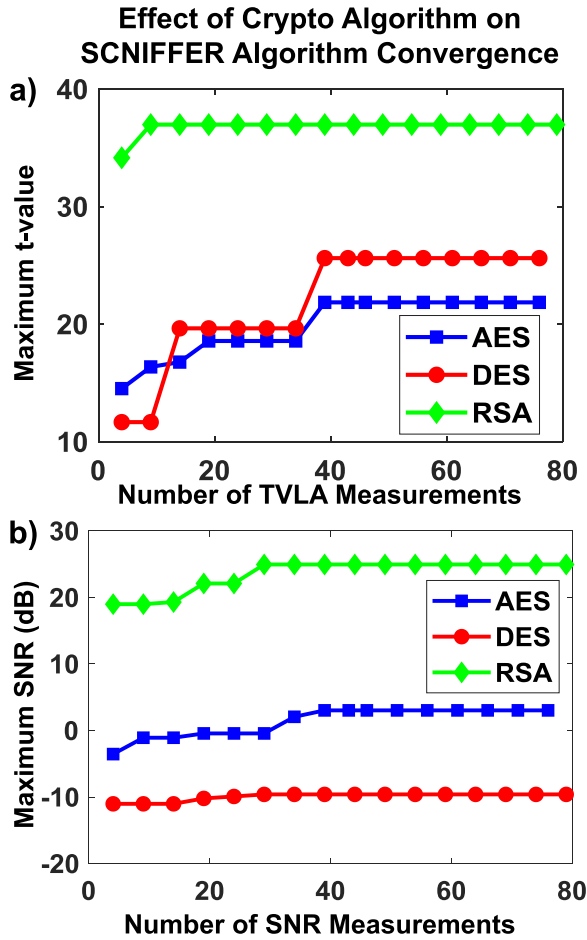


FIGURE 13. (a) Max t-value vs. number of TVLA tests performed for all cryptographic algorithms (AES, DES, RSA), showing the scanning algorithm performs well, finding the point of max leakage within 40 TVLA tests in all cases, with a grid size of 30×30 . The initial sampling grid was 2×2 and the step size was 0.84mm. Note that for RSA, one of the initial samples is already close to the maximum, and this maximum is found in just one step. For AES and DES, whose leakage patterns are less smooth, and have smaller areas of high leakage, the time to converge is higher. (b) Max SNR vs. number of SNR measurements for all algorithms (AES, DES, RSA). The search algorithm again performs well, converging in all cases in about $O(N)$ measurements ($N = 30$ in this case).

algorithms, and the parameters were fixed at a 2×2 starting grid and step size of 0.54 mm for all cases. A similar plot, using the same parameters but SNR as opposed to TVLA can be seen in Figure 13(b). Again, the search converges in approximately the same number of measurements for all algorithms. Through this, we see that the greedy gradient search algorithm performs well regardless of the specific cryptographic algorithm, and regardless of the leakage measure chosen.

E. EFFECT OF ARCHITECTURE ON CONVERGENCE

Additionally, we investigate the effect of different architectures (microcontrollers) on SCNIFFER. Up to now, the results shown have been obtained with an 8-bit XMEGA microcontroller. We now use a 32-bit STM32F3 microcontroller running software AES as the target device.

Effect of Architecture on SCNIFFER Algorithm Convergence

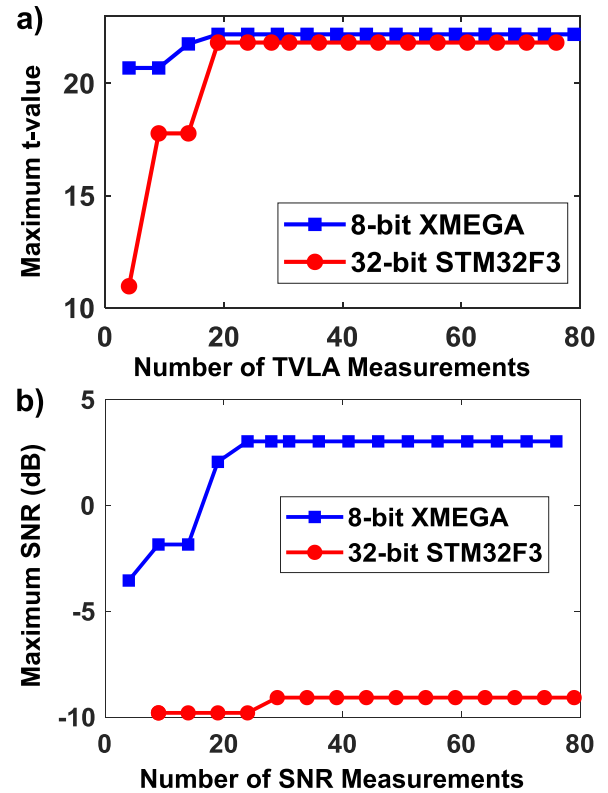


FIGURE 14. (a) Max t-value vs. number of measurements for both the 8-bit XMEGA microcontroller and the 32-bit STM32F3 microcontroller. The algorithm converges within $O(N)$ measurements, where $N = 30$ in both cases. The algorithm parameters used are the same as in Figure 13. (b) Max SNR vs. number of measurements for both microcontroller architectures, again showing convergence in $O(N)$ measurements. The parameters used are the same as those in part (a).

The STM32F3 uses the same clock frequency as the 8-bit XMEGA, 7.37MHz, and sampling is again done at $4 \times$ this frequency. Similarly the amplifier gain is the same as the 8-bit case. Given the same parameters for the greedy gradient search, the algorithm converges to a location of high leakage within N measurements, with $N = 30$ in this case. These results are shown in Figure 14(a) for TVLA, and Figure 14(b) for SNR. In both figures, the 8-bit and 32-bit architectures are compared, given the same measurement and search algorithm parameters. In this context, it is worth mentioning that as the size of the chip under attack increases, finding the location of the cryptographic engine could be a difficult task. In scenarios such as attacking large systems, the SCNIFFER framework would be extremely useful in efficiently determining the position of high leakage and then performing the attack at that point.

F. EFFECT OF MASKING ON CONVERGENCE

Lastly, the effects of a masking countermeasure with a fixed mask on the performance of SCNIFFER have been investigated. The same 8-bit XMEGA microcontroller was

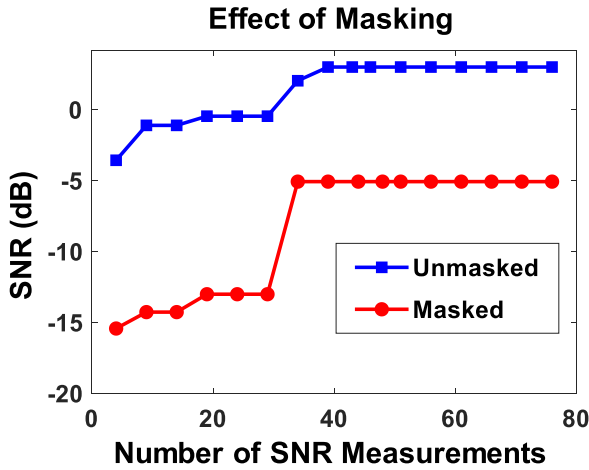


FIGURE 15. Max SNR vs. number of SNR measurements for the unmasked and a masked implementation of AES on the 8-bit microcontroller. The algorithm converges within $O(N)$ measurements, where $N = 30$ in both cases. The algorithm parameters used are the same as in Figure 13.

TABLE 5. Summary of SCNIFFER convergence for investigated algorithms, architectures, and countermeasures.

	AES	DES	RSA	AES - 32 bit	AES - Masked
Steps to Converge	39	29	29	29	34
Maximum SNR (dB)	3.02	-9.61	24.94	-9.08	-5.06

used as the target device, now running the masked implementation of AES-128 from [29]. We again use the same measurement and search parameters, and for both cases, the SCNIFFER algorithm converges in approximately $O(N)$ measurements. These results are shown in figure 15, where we see the algorithm converges after 35-40 measurements for both masked and unmasked implementations. As one would expect, the SNR for the masked implementation is significantly lower than the unmasked implementation, but the SCNIFFER search algorithm is still able to locate a higher SNR region through gradient search. While the measurement parameters used here were the same as elsewhere, an important note is that for countermeasures that reduce the SNR more drastically, would require more traces to be used to calculate the SNR. Table 5 summarizes the convergence results of the SCNIFFER search algorithm for all investigated algorithms, architectures, and the masking countermeasure. Note that RSA has a much higher SNR because the operations performed are different from a 0 bit vs. a 1 bit (for insecure implementations such as the one investigated, one can often classify bits from the EM leakage manually), whereas in AES/DES, the operations are the same and leakage is due to the actual data being processed. Consequently, there are only two classes considered in the case of RSA (0 or 1) compared to AES/DES which consider 9 classes (in the HW/HD models). For 32-bit AES, SNR is reduced as algorithmic

noise is increased due to more parallel operations leading to higher uncorrelated signals on the data bus. Even with these variations, SCNIFFER is able to find high leakage locations in approximately $O(N)$ measurements.

VII. CONCLUSION

This work has introduced SCNIFFER, a fully automated integrated system for conducting end-to-end EM side-channel attacks against cryptographic systems. SCNIFFER combines an EM leakage scanning platform, and correlation EM analysis into a single system, which can perform all steps of an attack automatically. The system is comprised of a low-cost custom scanning hardware and gradient search heuristic based scanning algorithm. We also plan to make our code for implementing the efficient SCNIFFER framework and controlling the low-cost 3-D printer for scanning publicly available.

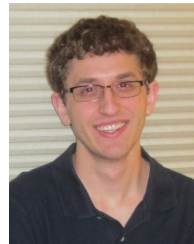
SCNIFFER is capable of using a variety of measures of leakage, and the search algorithm was shown to find a location of high leakage in an $N \times N$ chip search space with $O(N)$ measurements, providing a significant improvement over exhaustive search, and performing all stages of the search and attack completely automatically, removing the need for expert analysis.

Using this fully automated attack, it is possible to efficiently find a point of high leakage and launch a CEMA attack at this location at the press of a button. The attack uses a minimal number of traces, for a variety of microcontroller architectures and cryptographic algorithms. Even as the size of the chip increases, or as protections lowering the SNR, such as masking, are put in place, SCNIFFER retains efficiency. Finally, we show that as the SNR of the system under attack decreases, SCNIFFER attacks maintain their advantage over existing methods, reducing the number of traces needed by a factor of N compared to an exhaustive search, for an $N \times N$ scan of a chip.

REFERENCES

- [1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology (Lecture Notes in Computer Science)*, M. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 388–397.
- [2] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems (Lecture Notes in Computer Science)*, C. K. Koç, D. Naccache, and C. Paar, Eds. Berlin, Germany: Springer, 2001, pp. 251–261.
- [3] J.-J. Quisquater and D. Samyde, "Electro magnetic analysis (EMA): Measures and counter-measures for smart cards," in *Smart Card Programme Security (Lecture Notes in Computer Science)*, I. Attali and T. Jensen, Eds. Berlin, Germany: Springer, 2001, pp. 200–210.
- [4] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STEL-LAR: A generic EM side-channel attack protection through grounded root-cause analysis," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Los Alamitos, CA, USA, May 2019, pp. 11–20, doi: [10.1109/hst.2019.8740839](https://doi.org/10.1109/hst.2019.8740839).
- [5] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Cryptographic Hardware and Embedded Systems*, T. Güneysu and H. Handschuh, Eds. Berlin, Germany: Springer, 2015, pp. 207–228.
- [6] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Proc. RSA Conf. Topics Cryptol.-(CT-RSA)*, vol. 9610. New York, NY, USA: Springer-Verlag, 2016, pp. 219–235, doi: [10.1007/978-3-319-29485-8_13](https://doi.org/10.1007/978-3-319-29485-8_13).

- [7] A. Matthews, "Low cost attacks on smart cards," Next Gener. Secur. Softw., Manchester, U.K., Tech. Rep., 2006. [Online]. Available: <https://pdfs.semanticscholar.org/1b5a/48426397d3e5d7d56b35ffe2d8456e29834e.pdf>
- [8] T. Kasper, D. Oswald, and C. Paar, "EM side-channel attacks on commercial contactless smartcards using low-cost equipment," in *Information Security Application* (Lecture Notes in Computer Science), H. Y. Youm and M. Yung, Eds. Berlin, Germany: Springer, 2009, pp. 79–93.
- [9] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 195–212. [Online]. Available: <http://ieeexplore.ieee.org/document/7958578/>
- [10] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM side—Channel(s)," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), B. S. Kaliski, C. K. Koã, and C. Paar, Eds. Berlin, Germany: Springer, 2002, pp. 29–45.
- [11] C. Ramsay and J. Lohuis, "Tempest attacks against AES," Fox-IT, Fremont, CA, USA, Tech. Rep., 2017. [Online]. Available: <https://hardware.io/document/slides-craig-ramsay.pdf>
- [12] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), M. Joye and J.-J. Quisquater, Eds. Berlin, Germany: Springer, 2004, pp. 16–29.
- [13] G. Becker, "Test vector leakage assessment (TVLA) methodology in practice," in *Proc. Int. Cryptograph. Module Conf.*, vol. 1001, 2013, p. 13.
- [14] S. Mangard, "Hardware countermeasures against DPA—A statistical analysis of their effectiveness," in *Topics Cryptology* (Lecture Notes in Computer Science), T. Okamoto, Ed. Berlin, Germany: Springer, 2004, pp. 222–235.
- [15] Y. Liu and B. Ravelo, "Fully time-domain scanning of EM near-field radiated by RF circuits," *Prog. Electromagn. Res.*, vol. 57, pp. 21–46, Apr. 2014.
- [16] V. Lomnã, P. Maurine, L. Torres, T. Ordas, M. Lisart, and J. Toubanc, "Modeling time domain magnetic emissions of ICs," in *Integrated Circuit and System Design. Power and Timing Modeling, Optimization, and Simulation* (Lecture Notes in Computer Science), R. van Leuken and G. Sicard, Eds. Berlin, Germany: Springer, 2011, pp. 238–249.
- [17] L. Sauvage, S. Guilley, and Y. Mathieu, "Electromagnetic radiations of FPGAs: High spatial resolution cartography and attack on a cryptographic module," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 2, no. 1, pp. 1–24, Mar. 2009.
- [18] J. Heyszl, D. Merli, B. Heinz, F. De Santis, and G. Sigl, "Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis," in *Int. Conf. Smart Card Res. Adv. Appl.*, 2012, pp. 248–262.
- [19] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of cryptographic implementations," in *Topics Cryptology* (Lecture Notes in Computer Science), O. Dunkelmann, Ed. Berlin, Germany: Springer, 2012, pp. 231–244.
- [20] R. Specht, V. Immler, F. Unterstein, J. Heyszl, and G. Sigl, "Dividing the threshold: Multi-probe localized EM analysis on threshold implementations," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Apr. 2018, pp. 33–40.
- [21] F. Unterstein, J. Heyszl, F. De Santis, and R. Specht, "Dissecting leakage resilient PRFS with multivariate localized em attacks," in *Proc. Int. Workshop Constructive Side-Channel Anal. Secure Des.*, 2017, pp. 34–49.
- [22] V. V. Iyer and A. E. Yilmaz, "An adaptive acquisition approach to localize electromagnetic information leakage from cryptographic modules," in *Proc. IEEE Texas Symp. Wireless Microw. Circuits Syst. (WMCS)*, Mar. 2019, pp. 1–6.
- [23] *EM Probe Station: Electromagnetic Analysis Solution*. Accessed: Jun. 29, 2019. [Online]. Available: <https://www.riscure.com/product/em-probe-station/>
- [24] *Crealitiy3d Ender-3 3D Printer Economic Ender DIY KITS*. Accessed: Jun. 29, 2019. [Online]. Available: <https://www.crealitiy3d.shop/products/creality3d-ender-3-pro-high-precision-3d-printer>
- [25] C. O'Flynn and Z. D. Chen, "ChipWhisperer: An open-source platform for hardware embedded security research," in *Constructive Side-Channel Anal. Secure Design* (Lecture Notes in Computer Science), E. Prouff, Ed. Cham, Switzerland: Springer, 2014, pp. 243–260.
- [26] O.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proc. IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006. [Online]. Available: <https://ieeexplore.ieee.org/document/1580507>
- [27] D. B. Roy, S. Bhasin, S. Guilley, A. Heuser, S. Patranabis, and D. Mukhopadhyay, "CC meets FIPS: A hybrid test methodology for first order side channel analysis," *IEEE Trans. Comput.*, vol. 68, no. 3, pp. 347–361, Mar. 2019.
- [28] D. B. Roy, S. Bhasin, S. Guilley, A. Heuser, S. Patranabis, and D. Mukhopadhyay, (2016). *Leak Me if You Can: Does TVLA Reveal Success Rate*. [Online]. Available: <https://eprint.iacr.org/2016/1152>
- [29] R. Benadjila, V. Lomnã, E. Prouff, and T. Roche. (2017). *Secure AES128 on ATMEGA8515*. [Online]. Available: <https://github.com/ANSI-SI-FR/secAES-ATmega8515>



JOSEF DANIAL (Student Member, IEEE) received the B.Sc. degree in computer engineering from Purdue University, West Lafayette, IN, USA, in 2018, where he is currently pursuing the master's degree with the SPARC Laboratory. He has two years of industry experience, in automotive (Fiat Chrysler Automobiles) and IoT (Cisco Jasper) companies. He is also a Graduate Research Assistant with Purdue University. His research interests include machine learning, hardware security, and computer vision.



DEBAYAN DAS (Member, IEEE) received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, India, in 2015. He is currently pursuing the Ph.D. degree with the SPARC Laboratory, Purdue University, USA. From 2015 to 2016, he worked as an Analog Design Engineer with xSi Semiconductors (start-up). His research interests include hardware security and mixed-signal IC design. He was a recipient of the IEEE HOST Best Student Paper Award,

in 2017 and 2019, and the 3rd Best Poster Award in IEEE HOST 2018. In 2019, one of his papers was recognized as a Top Pick in Hardware & Embedded Security published over the span of last six years. He has been awarded the ECE Fellowship during 2016–18 and the Bilsland Dissertation Fellowship during the final year (2020–21) for his outstanding overall achievements.



SANTOSH GHOSH (Member, IEEE) received the Ph.D. degree from the Department of Computer Science and Engineering, IIT Kharagpur, in 2011. He was a Postdoctoral Researcher with COSIC, KU Leuven. He is currently with Intel Labs, Intel Corporation, Hillsboro, OR, USA. He has over 40 research publications and 35 filed patents in USA. His research interests include cryptography, hardware security, security for IoT, and autonomous driving.



ARIJIT RAYCHOWDHURY (Senior Member, IEEE) received the B.E. degree in electrical and telecommunication engineering from Jadavpur University, India, in 2001, and the Ph.D. degree in electrical and computer engineering from Purdue University, in 2007.

From 2013 to July 2019 he was an Associate Professor and held the ON Semiconductor Junior Professorship with the department. He was a Staff Scientist with the Circuits Research Laboratory,

Intel Corporation. He was an Analog Circuit Researcher with Texas Instruments Inc. He is currently a Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology. He is also the Co-Director of the Georgia Tech Quantum Alliance. His significant contributions to the semiconductor industry include the design of the world's first adaptive echo-cancellation network for integrated DSLs (TI) and embedded world-line boosting for SRAM arrays (Intel). He has published over 170 papers in journals and refereed conferences. He holds more than 25 U.S. and international patents. His research interests include low power digital and mixed-signal circuit design, design of power converters, sensors, and exploring interactions of circuits with device technologies. He has served on the Technical Program Committees of VLSI Symposium, CICC, DAC, ICCAD, ISLPED, and DATE. From 2013 to 2018, he was an Associate Editor of the IEEE TRANSACTIONS ON COMPUTER AIDED DESIGN. From 2013 to 2017, he was an Editor of *Microelectronics Journal* (Elsevier). He has also been a guest editor for multiple IEEE and ACM journals. He has also taught many short courses and invited tutorials at multiple conferences, workshops, industries, and universities. He is the winner of the IEEE/ACM Innovator under 40 award, the NSF CISE Research Initiation Initiative Award (CRII), in 2015, the Intel Labs Technical Contribution Award, in 2011, the Dimitris N. Chorafas Award for Outstanding Doctoral Research, in 2007, the Best Thesis Award, College of Engineering, Purdue University, in 2007, the SRC Technical Excellence Award, in 2005, the Intel Foundation Fellowship, in 2006, the NASA INAC Fellowship, in 2004, and the Meissner Fellowship, in 2002. He and his students have won eleven best paper awards over the years.



SHREYAS SEN (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the Georgia Tech, Atlanta, GA, USA, in 2011.

He is currently an Assistant Professor with the School of Electrical and Computer Engineering, Purdue University. He has over five years of industry research experience with Intel Labs, Qualcomm and Rambus. He has authored/coauthored two book chapters and over 120 conference and

journal papers. He has 13 patents granted/pending. His research interests include mixed-signal circuits/systems for the Internet of Things (IoT), biomedical, and security. He was an Executive Committee Member of the IEEE Central Indiana Section, ETS. He was a Technical Program Committee Member of DAC, CICC, DATE, ISLPED, ICCAD, ITC, VLSI Design, IMSTW, and VDAT. In 2018, he was chosen by MIT Technology Review as one of the top ten Indian Inventors Worldwide under 35 (MIT TR35 India Award), for the invention of using the Human Body as a Wire, which has the potential to transform healthcare, neuroscience, and human-computer interaction. He was a recipient of the AFOSR Young Investigator Award 2017, the NSF CISE CRII Award 2017, the Google Faculty Research Award 2017, the HKN Outstanding Professor Award, the Intel Labs Divisional Recognition Award 2014 for industry-wide impact on USB-C type, the Intel PhD Fellowship 2010, the IEEE Microwave Fellowship 2008, the GSRC Margarida Jacome Best Research Award 2007, the Best Paper Awards at CICC 2019, the HOST 2017, 2018, and 2019, the ICCAD Best-in-Track Award 2014, the VTS Honorable Mention Award 2014, the RWS Best Paper Award 2008, the Intel Labs Quality Award 2012, the SRC Inventor Recognition Award 2008, and the Young Engineering Fellowship 2005. He serves/has served as an Associate Editor for the IEEE DESIGN & TEST.

...