ADVANCED EM/POWER SIDE-CHANNEL ATTACKS AND LOW-OVERHEAD CIRCUIT-LEVEL COUNTERMEASURES

by

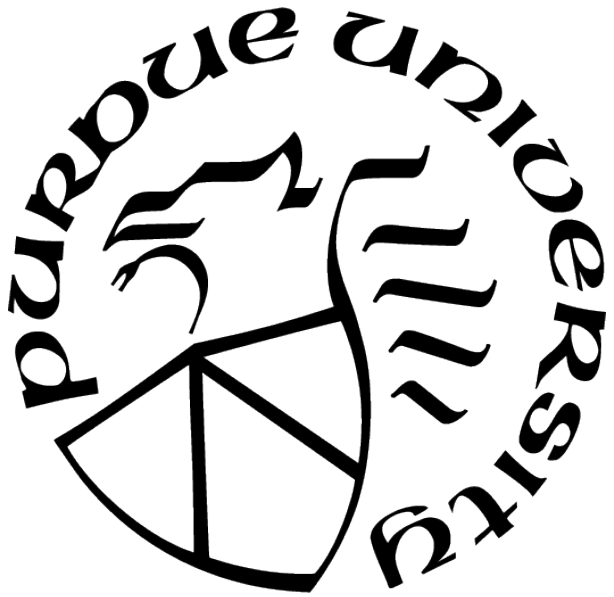
Debayan Das

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy



School of Electrical and Computer Engineering

West Lafayette, Indiana

August 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Shreyas Sen, Chair

School of Electrical and Computer Engineering

Dr. Kaushik Roy

School of Electrical and Computer Engineering

Dr. Anand Raghunathan

School of Electrical and Computer Engineering

Dr. Vijay Raghunathan

School of Electrical and Computer Engineering

Dr. Santosh Ghosh

Security & Privacy Research, Intel Labs, OR, USA

Approved by:

Prof. Dimitrios Peroulis

Dedicated to my loving parents who have sacrificed immensely
to make me what I am today.
Mrs. Babita Das and Dr. Utpal Das

ACKNOWLEDGMENTS

There are numerous people to whom I am highly grateful for my successes. First and foremost, I am extremely thankful to my advisor and guide Prof. Shreyas Sen for giving me this wonderful opportunity for the last five years. It has been an exciting journey with a lot of ups and downs and I am glad that I have been able to withstand all of that. I am very grateful to Prof. Shreyas for his words of encouragement before my conference presentations, which resulted in multiple best paper awards. He has always encouraged me to strive for the best. I have been fortunate enough to have received multiple fellowships and distinctions, and Prof. Shreyas has been a major source of inspiration through all of these.

I would also like to thank all other professors in my thesis committee Prof. Anand Raghunathan, Prof. Kaushik Roy, and Prof. Vijay Raghunathan for their guidance and support during my PhD. My thanks also to Dr. Santosh Ghosh from Intel Labs for his tremendous support as my committee member.

I am sincerely thankful to all of my present colleagues and alumni in the SPARC Lab, Dr. Shovan Maity, Baibhab Chatterjee, Mayukh Nath, Donghyun Seo, Nirmoy Modak, Josef Danial, David Yang, Archisman Ghosh, Gaurav Kumar K, Arunashis Dutta, Faizul Bari, Austyn Krutsinger, Gregory Chang, Parikha Mehrotra, Jie Yang, Yudhajit Ray, Kurian Polachan, John Gerguis, Shitij Avlani, Shreeya Sriram, Rohan Manna, Dr. Abhishek Srivastava for their help with my work and collaboration. I enjoyed the congenial atmosphere created in the lab which allowed for many insightful discussions.

I am also grateful to other research group members including Hengying Shan, John Peterson, Dr. Arnab Raha, Dr. Mohit Singh, as well as Dr. Mark Johnson for their help and assistance during my PhD. I would like to thank Anupam Golder, Muya Chang, Saad Bin Nasir (Georgia Tech), and Jeremy Blackstone (UC San Diego) for exciting collaborative research during my PhD.

I am extremely proud and thankful to have worked with many inspiring collaborators across universities including Prof. Arijit Raychowdhury, Prof. Ryan Kastner, Prof. Ingrid Verbauwhede, Prof. Kanad Basu, Prof. Visvesh Sathe. I am also sincerely thankful to Prof. Swarup Bhunia, Prof. Mark Tehranipoor for their help and support during my PhD.

I would like to thank Intel Corporation for funding my PhD research and also providing me the opportunity to do two summer internships. I am extremely grateful to my mentor Dr. Santosh Ghosh and my other collabortors at Intel, Dr. Sanu Mathew, Dr. Harish Krishnamurthy, Dr. Carlos Tokunaga, Dr. Xiaosen Liu, Dr. Raghavan Kumar, Dr. Avinash Varna, Dr. Anand Rajan, and Dr. Manoj Sastry for their feedback and suggestions regarding my research works.

I am immensely thankful to my close friends, Dr. Shovan Maity, Baibhab Chatterjee, Mayukh Nath, Donghyun Seo, Nirmoy Modak, Josef Danial, Archisman Ghosh, Gaurav Kumar K, Arunashis Dutta, Indranil Chakraborty, Deboleena Roy, Sibendu Paul, Sourav Sanyal, Gargi Bhattacharya, Soumyadeep Chandra for their unconditional help and making my PhD life enjoyable. I am highly grateful to Anindita Das for her support and encouragement over the last five years. I would also like to thank my girlfriend Priyanka Naskar for being extremely supportive and understanding through many tough times over the last two years.

Finally, I am highly indebted towards my parents, Dr. Utpal Das and Mrs. Babita Das for their unflinching love and support throughout. They not only pushed me towards achieving my dreams and pursuing a career in research, but also greatly strived towards making me a better person. I dedicate this thesis to them.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The huge gamut of today's internet-connected embedded devices has led to increasing concerns regarding the security and confidentiality of data. To address these requirements, most embedded devices employ cryptographic algorithms, which are computationally secure. Despite such mathematical guarantees, as these algorithms are implemented on a physical platform, they leak critical information in the form of power consumption, electromagnetic (EM) radiation, timing, cache hits and misses, and so on, leading to side-channel analysis (SCA) attacks. Non-profiled SCA attacks like differential/correlational power/EM analysis (DPA/CPA/DEMA/CEMA) are direct attacks on a single device to extract the secret key of an encryption algorithm. On the other hand, profiled attacks comprise of building an offline template (model) using an identical device and the attack is performed on a similar device with much fewer traces.

This thesis focusses on developing efficient side-channel attacks and circuit-level low-overhead generic countermeasures. A cross-device deep learning-based profiling power side-channel attack (X-DeepSCA) is proposed which can break the secret key of an AES-128 encryption engine running on an Atmel microcontroller using just a single power trace, thereby increasing the threat surface of embedded devices significantly. Despite all these advancements, most works till date, both attacks as well as countermeasures, treat the crypto engine as a black box, and hence most protection techniques incur high power/area overheads.

This work presents the first white-box modeling of the EM leakage from a crypto hardware, leading to the understanding that the critical correlated current signature should not be passed through the higher metal layers. To achieve this goal, a signature attenuation hardware (SAH) is utilized, embedding the crypto core locally within the lower metal layers so that the critical correlated current signature is not passed through the higher metals, which behave as efficient antennas and its radiation can be picked up by a nearby attacker. Combination of the 2 techniques – current-domain signature suppression and local lower metal routing shows $> 350\times$ signature attenuation in measurements on our fabricated 65nm test chip, leading to SCA resiliency beyond 1B encryptions, which is a $100\times$ improvement

in both EM and power SCA protection over the prior works with comparable overheads. Moreover, this is a generic countermeasure and can be utilized for any crypto core without any performance degradation.

Next, backed by our physics-level understanding of EM radiation, a digital library cell layout technique is proposed which shows $> 5\times$ reduction in EM SCA leakage compared to the traditional digital logic gate layout design. Further, exploiting the magneto-quasistatic (MQS) regime of operation for the present-day CMOS circuits, a HFSS-based framework is proposed to develop a pre-silicon EM SCA evaluation technique to test the vulnerability of cryptographic implementations against such attacks during the design phase itself.

Finally, considering the continuous growth of wearable and implantable devices around a human body, this thesis also analyzes the security of the internet-of-body (IoB) and proposes electro-quasistatic human body communication (EQS-HBC) to form a covert body area network. While the traditional wireless body area network (WBAN) signals can be intercepted even at a distance of $5m$, the EQS-HBC signals can be detected only up to $0.15m$, which is practically in physical contact with the person. Thus, this pioneering work proposing EQS-HBC promises $> 30\times$ improvement in private space compared to the traditional WBAN, enhancing physical security. In the long run, EQS-HBC can potentially enable several applications in the domain of connected healthcare, electroceuticals, augmented and virtual reality, and so on. In addition to these physical security guarantees, side-channel secure cryptographic algorithms can be augmented to develop a fully secure EQS-HBC node.

1. INTRODUCTION

1.1 Background of Side-channel analysis (SCA)

1.1.1 IoT Security

Cyber-physical systems are inter-connected or networked embedded systems interacting with the environment. The core of the cyber-physical system is the cloud which provides the necessary infrastructure to perform big data analysis. In the next level, we have the computers and laptops, which still have a good amount of resources. Finally, there are edge devices like smartwatches, smartphones, ear pods, SpO2 sensors, fitness trackers, or even pacemakers, which are typically resource-constrained and forms the internet of things (IoT) [1]. The Internet of Things (IoT) has been expanding continuously and is forecasted to reach a $10 trillion economy by 2025 [2].

As the size of unit computing reduces and more smart devices are becoming part of this IoT network [3], [4], [5], [6], [7], these devices need to be extremely resource-constrained (RC) [8], [9], [10], [11], [12]. Now with the growing inter-connected RC-IoT devices, one weak point of entry in this network might spread catastrophically over large areas leaking confidential information to the attacker [13]. Due to the energy, memory and compute capacity constraints, traditional security measures (for example, generating a session key through public key encryption) are not always applicable in RC-IoT nodes [9]. Recently, internet-of-body (IoB) has emerged as a new paradigm which consists of wearable and implantable devices in and around the human body [14], [15], [16], [17],. Resource-constrained IoB (RC-IoB) devices like insulin pumps or pacemakers are also vulnerable to many security vulnerabilities [18]. Today, there are 50B connected IoT and IoB devices, and the numbers are only increasing leading to smart homes and smart cars. However, none of these are smart without the security of these devices. This has led to the growing cybersecurity market, which is worth billions of dollars today (Fig. 1.1). Now, these IoT/IoB devices, when in possession of an attacker becomes extremely vulnerable to physical side-channel analysis attacks.

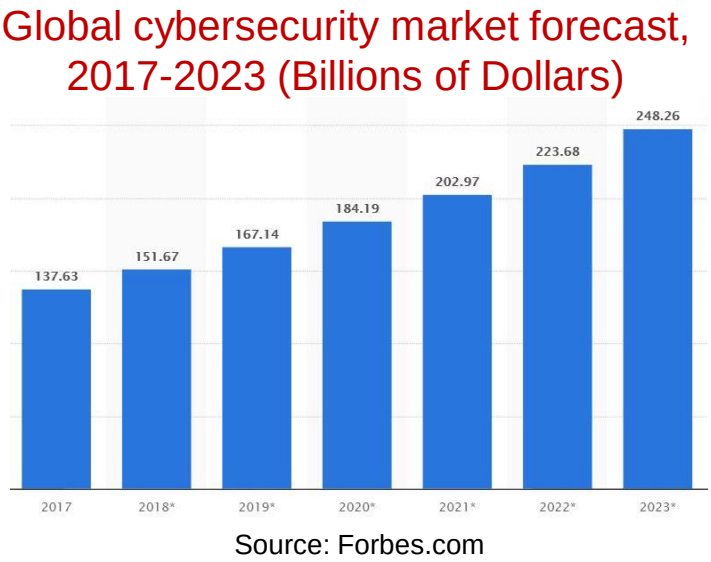


Figure 1.1. Cybersecurity market forecast

1.1.2 EM Hardware Security

Any device implemented on a physical substrate starts radiating through the EM emanations. Such EM radiations can be used for both attacks to recover the secret cryptographic key as well as in forensics and malware detection. In the domain of hardware security, we have also seen a rise in the development of physically unclonable functions (PUFs) which can be utilized for device authentication using physical radio frequency (RF) signatures [19], [20], [21]. EM signatures have been used to monitor the program execution at the granularity of instructions, showing that we can distinguish between different operations like load and store to memory, or distinguishing the divide instruction from multiplication or addition operation [22]. Spectral profiling was utilized to recognize periodic loop activities and its runtime, leading to malware detection using the EM signatures [23]. Recently, backscattering side-channel using EM signature was introduced, which is used to detect hardware trojans or counterfeiting of ICs [24].

Many real-world exploits utilizing power and electromagnetic side-channel analysis have been demonstrated. Recently, the smart lighting system Philips Hue was hacked recently by exploiting the underlying operating system, utilizing what is known as power side-channel analysis [13], allowing the attacker to perform over-the-air firmware updates. Recent dis-

- **Physical Possession**
  - Same Static Key for all devices → break one attack any
    - Counterfeit e-cigarettes, Philips Hue attack
  - Distinct Static Keys (i.e. no Session Key) → all data/messages are recovered
    - Google Titan Security Key
    - iPhone key recovery
  - Distinct Time-varying Session Keys → information of one session only
- **Remote Attack through Physical Coupling**
  - Distinct Time-varying Session Keys → information of one session only
    - Software-based attacks on Intel/AMD processors through the Running Average Power Limit (RAPL) interface
  - Multi-Tenant FPGA Ring Oscillator based attack through Power Coupling
  - EM-Attack from Next Room

Figure 1.2. SCA attack application scenarios.

tributed denial of service (DDoS) attack by the Dyn DNS company demonstrated taking control over millions of inter-connected webcams [25]. These attacks only show a small subset of the wide range of vulnerabilities in many of the existing commercial resource-constrained IoT devices.

1.1.3 Side-Channel Analysis

The growth of these low-cost resource-constrained internet-connected (IoT) devices is of immense interest from a security perspective. As the systems become increasingly complex, more potentially exploitable attack vectors emerge, leading to higher chances of security vulnerabilities.

Hence, most of today's embedded devices are equipped with cryptographic algorithms to provide confidentiality and authenticity of data. However, these algorithms are implemented on a physical substrate, which leak critical correlated information in the form of electromagnetic (EM) radiation, power consumption, timing of the crypto operations, cache hits and misses, and so on, leading to side-channel analysis (SCA) attacks. An attacker can utilize this side-channel leakage information to extract the secret key.

As multiple devices remain inter-connected within an IoT network, a small vulnerability on one of the edge devices could prove extremely costly to the security of the entire large-scale network. The different SCA attack application scenarios are shown in Fig. 1.2. The attacks can be classified as remote and physical. For the physical possession category of attacks, it can be further classified into 3 classes. Firstly, for devices having the same static key for all devices, some of the real-world attacks include counterfeiting of e-cigarette batteries, and the attack on the Phillips Hue smart bulbs [13]. In this case, once a device is compromised, all other devices are also compromised. For the second class of devices with distinct static keys (without generation of session key, that is, no public key encryption), the particular device under attack is only compromised. Real-world examples of this class include the attack on Google Titan Security Key [26], and key extraction from iPhone devices utilizing EM SCA [27]. In the final class of devices are the ones with varying session keys, from which information from only one session can be extracted. Now, the remote SCA attacks include software-based attacks on high performance Intel computing platforms utilizing the running average power limit (RAPL) interface to extract the AES as well as RSA keys from the software guard extension (SGX) enclave [28]. Moreover, with the advent of cloud computing, multi-tenant FPGAs are being attacked utilizing ring oscillators through the power coupling [29], [30], [31]. Also, with the development of high gain antennas, we are seeing increased long-distance EM SCA attacks on embedded devices [32], [33].

The flow of a traditional non-profiled power/EM SCA attack is shown in Fig. 1.3. As the device is performing encryptions, traces are collected from the crypto engine corresponding to a set of chosen plaintexts or known ciphertexts (more practical assumption). Next, for the algorithm, a point of attack is determined, which is typically the first or last round for an AES implementation. Then, a hamming weight (HW) or a hamming distance (HD) model is computed for each key byte. The HW model counts the number of ones on the data bus, while the HD model computes the number of bits switching from one state to the next. The HD model is more practical and typically used for most hardware implementations (FPGAs/ASICs), while the HW model is a special case of the HD model and is mostly useful for software implementations which have a reset phase between each encryptions. Finally,

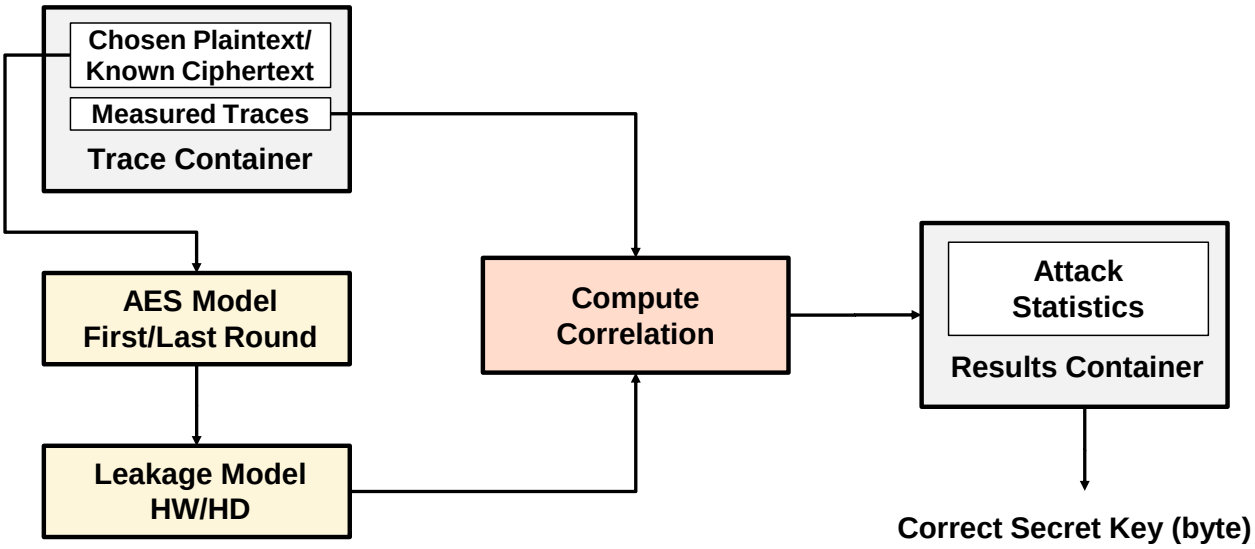


Figure 1.3. Flow of a traditional non-profiled SCA attack.

the measured power/EM SCA traces are correlated with the HW/HD model and the correct key byte emerges as multiple traces are analyzed.

Hence, security considerations including power and EM side-channel leakage analysis, should form a necessary part of the design life-cycle of all the embedded devices, even if it is not a critical node of the IoT network. Despite these requirements, many existing embedded devices do not employ SCA protection. This could be because of two main reasons: the time to market and the cost. Firstly, the time to market is extremely important for an industry and hence SCA attack protection schemes need to be scalable across technologies and should be generic for all algorithms. Moreover, it is desirable to have a countermeasure as a wrapper around the entire crypto core without any changes to the existing algorithms, thereby also ensuring legacy protection. Secondly, the cost is related to the area, power and throughput overheads of the countermeasure. Hence, a low-overhead energy-efficient generic synthesizable countermeasure is necessary which can provide protection against both EM as well as power SCA attacks. In this thesis, we perform a white-box analysis of the EM leakage to root-cause the source of the EM radiation from a crypto IC, leading to the design of a current domain signature attenuation (CDSA) hardware with local lower-level metal routing to protect against both EM as well as power SCA attacks.

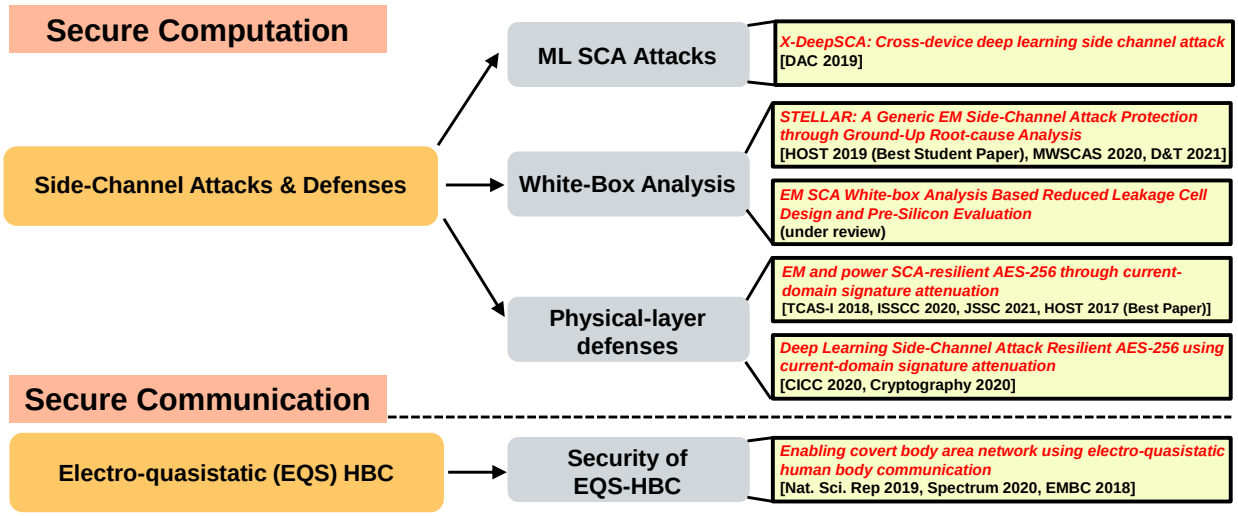


Figure 1.4. Overview of the thesis

1.2 Key Contributions of my thesis

The three main pillars for enabling a secure and efficient cyber-physical system are intelligence (compute), connectivity (communication), and security. In this dissertation, I have focused on both secure computation as well as secure communication. The outline of my dissertation is shown in Fig. 1.4.

1.2.1 Advanced Machine Learning based SCA attacks

On secure computation, I have proposed advanced deep-learning based cross-device side-channel attacks on encryption devices [34], [35], [36], which increased the threat surface for embedded devices significantly. This forms the Chapter 2 of this thesis.

1.2.2 White-box analysis of the EM SCA leakage

Next, a white-box analysis of the electromagnetic (EM) side-channel leakage is performed to understand the root-cause of the EM radiation from the integrated circuits (ICs). This forms the Chapter 3 of this thesis.

1.2.3 Reduced EM Leakage Cell Design and Pre-Silicon Evaluation

With a thorough understanding of the genesis of the EM leakage [37], [38], this thesis proposes a reduced EM leakage cell design along with a pre-silicon EM SCA evaluation framework [39]. This is presented in Chapter 4 of this thesis.

1.2.4 EM & Power SCA Countermeasure in 65nm CMOS

Equipped with this white-box understanding of the EM leakage from a crypto IC, physical-layer defenses are proposed in the circuit level, which achieves the highest side-channel security till date with low power and area overheads [40], [41], [42], [43], [44], [45], [46]. This is demonstrated in Chapter 5 of this thesis.

1.2.5 Evaluation of the Countermeasure against Deep Learning SCA

The proposed circuit to prevent both EM as well as power SCA attacks have been verified against the state-of-the-art machine-learning (ML) SCA attacks [47]. This is presented in Chapter 6 of this thesis.

1.2.6 Physical Security of Human Body Communication

Finally, my work pioneered and analyzed the security of electro-quasistatic human body communication (EQS-HBC) to transmit sensitive data at lower frequencies in the EQS regime so that the EM radiation is minimized & the physical security of HBC is maximized compared to the traditional fundamentally radiative wireless body area networks WBANs [48], [14], [49], [50], [51], [52], [53], [54], [55], [56], [57]. This forms the Chapter 7 in this thesis.

1.3 Thesis Organization

The thesis is organized as follows. First, in Chapter 2, we present the `X-DeepSCA` attack on an AES-128 encryption engine. Next, in Chapter 3, the root-cause analysis of the EM SCA leakage is investigated leading towards the our proposed STELLAR technique. Following this, Chapter 4 presents a reduced EM leakage cell design for SCA security, along with the

pre-silicon EM SCA evaluation framework. Chapter 5 presents a current domain signature attenuation hardware (CDSA), which is a low-overhead generic countermeasure with on-chip demonstration to prevent against both EM as well as power SCA attacks. Chapter 6 analyzes the deep-learning attack resilience of the CDSA countermeasure. In Chapter 7, we investigate the physical security properties of the EQS-HBC communication system. Finally, Chapter summarizes and concludes the thesis.

2. ADVANCED MACHINE LEARNING SCA ATTACKS ON EMBEDDED DEVICES

Most of the materials in this chapter have been extracted verbatim from the paper:
1. Debayan Das, Anupam Golder, Josef Danial, Santosh Ghosh, Arijit Raychowdhury, Shreyas Sen, `X-DeepSCA`: Cross-device deep learning side channel attack, *IEEE/ACM Design Automation Conference (DAC)*, 2019.

This work, for the first time, demonstrates Cross-device Deep Learning Side-Channel Attack (`X-DeepSCA`), achieving an accuracy of $> 99.9\%$, even in presence of significantly higher inter-device variations compared to the inter-key variations. Augmenting traces captured from multiple devices for training and with proper choice of hyper-parameters, the proposed 256-class Deep Neural Network (DNN) learns accurately from the power side-channel leakage of an AES-128 target encryption engine, and an N-trace ($N \leq 10$) `X-DeepSCA` attack breaks different target devices within seconds compared to a few minutes for a correlational power analysis (CPA) attack, thereby increasing the threat surface for embedded devices significantly. Even for low SNR scenarios, the proposed `X-DeepSCA` attack achieves $\sim 10\times$ lower minimum traces to disclosure (MTD) compared to a traditional CPA.

2.1 Background

This chapter focuses on the power SCA attacks. Non-profiled SCA attack techniques include differential and correlational power/EM analysis (DPA/CPA/DEMA/CPA), which have been utilized to break many real-world encryption devices [58]–[60]. These are direct attacks on encryption devices and requires thousands of traces to break an efficient crypto implementation. On the other hand, profiled SCA attacks comprise of two stages: profiling and attack [61]–[63]. In the profiling phase, multiple traces from an identical device are collected by varying sub-keys (part of the cryptographic key), and a model is built. The entire heavylifting is thus off-loaded to the training phase, which happens offline prior to the attack phase (Fig. 2.1). During the attack stage, the model is utilized to classify each

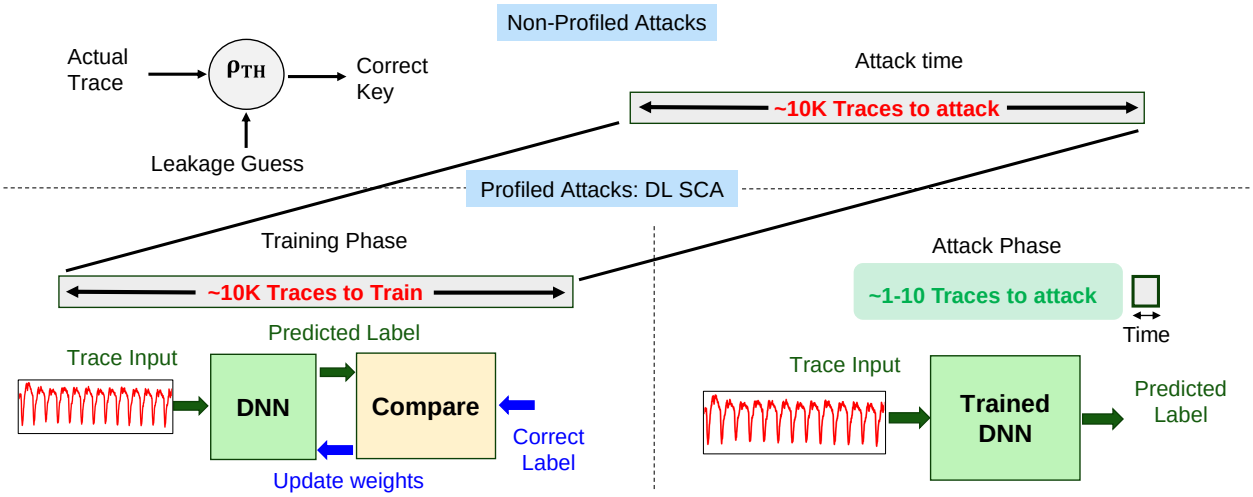


Figure 2.1. Summary of Non-profiled and Profiled Attacks

sub-key of the device under attack. The attack requires as low as a single trace to recover the correct key. The summary of the comparison of the non-profiled and profiled attacks is shown in Fig. 2.1.

In recent years, various machine-learning (ML) techniques have been evaluated to perform profiling power SCA attacks [64]–[66]. Although successful attacks have been shown, these ML techniques require pre-processing of the traces with proper time-alignment. In 2017, Cagli et al. [67] proposed a deep-learning based approach utilizing convolutional neural networks (CNNs) to provide an end-to-end profiling strategy, even in the presence of trace misalignments. Masking-based countermeasures were also shown to be broken using neural networks [68], [69]. Deep learning based SCA attacks does not require extensive statistical analysis to identify the points of leakage, in contrast to the template attacks. Also, as the dimensions of the data increase, ML SCA attacks become more prominent compared to the template attacks [65]. Deep Learning (DL) based SCA is still a new research paradigm [70] and all the **previous works till date have focused on evaluating and improving the attack on the same device** which has been used to train the neural network.

This work, for the first time, demonstrates a Cross-Device Deep Learning based Side-Channel Attack (`X-DeepSCA`) using a 256-class DNN. Figure 2.2(a) shows the measured cross-device variations in the form of a histogram (red plot) of the absolute difference between the

samples at the same time index of the averaged traces from 2 different devices (TR_1, D_1) running the same software implementation of AES-128. For the device TR_1, the green curve shows the histogram of the variation between 2 different key bytes (classes). We see that the *inter-device variations for the same key are significantly higher than the inter-key variations of the same device*, which makes the cross-device attack particularly challenging. The confusion matrices in Figure 2.2(b) show that although the test accuracy on the same device (DNN trained with device TR_1 and tested with unseen traces from the same device) is very high (red dots represent the misclassified key bytes), the accuracy on a different test device (D_1) is significantly lower. Hence, training with one profiling device overfits to that particular device leakage and may not be able to generalize well to other devices.

Hence, in this work, we augment traces from multiple profiling devices (Figure 6.1(b)) and build a DNN architecture to perform cross-device deep-learning based power side-channel analysis (`X-DeepSCA`) attack. In addition, we analyze the individual class (key byte) accuracies and demonstrate the practicality of an N-trace ($N \leq 10$) `X-DeepSCA` attack to achieve $> 99.9\%$ success of attack. Finally, we study the effect of varying SNR scenarios, and show that the `X-DeepSCA` attacks require $\sim 10\times$ lower number of traces to attack (minimum traces to disclosure: MTD) than the traditional correlation power analysis (CPA) attacks [71].

In summary, the key contributions of this work are:

- A combination of designing the appropriate 256-class DNN with proper choice of the hyperparameters to prevent overfitting, utilizing traces from multiple devices (TR_{1-4}) during training, coupled with the proposed N-trace attack leads to the first successful demonstration of a cross-device deep-learning SCA (`X-DeepSCA`) attack.

- Using the Keras library with a Tensorflow backend [72], we show that the single-trace `X-DeepSCA` attack using the DNN model achieves an average accuracy of $> 99.9\%$ for all the test devices (D_{1-4}) under attack using 200K total traces for the training (Sec. 3).

- Further, we investigate the individual class accuracies by introducing a measure of entropy, leading to the proposed N-trace `X-DeepSCA` attack to guarantee $> 99.9\%$ attack success with $N \leq 10$ encryptions (Sec. 4).

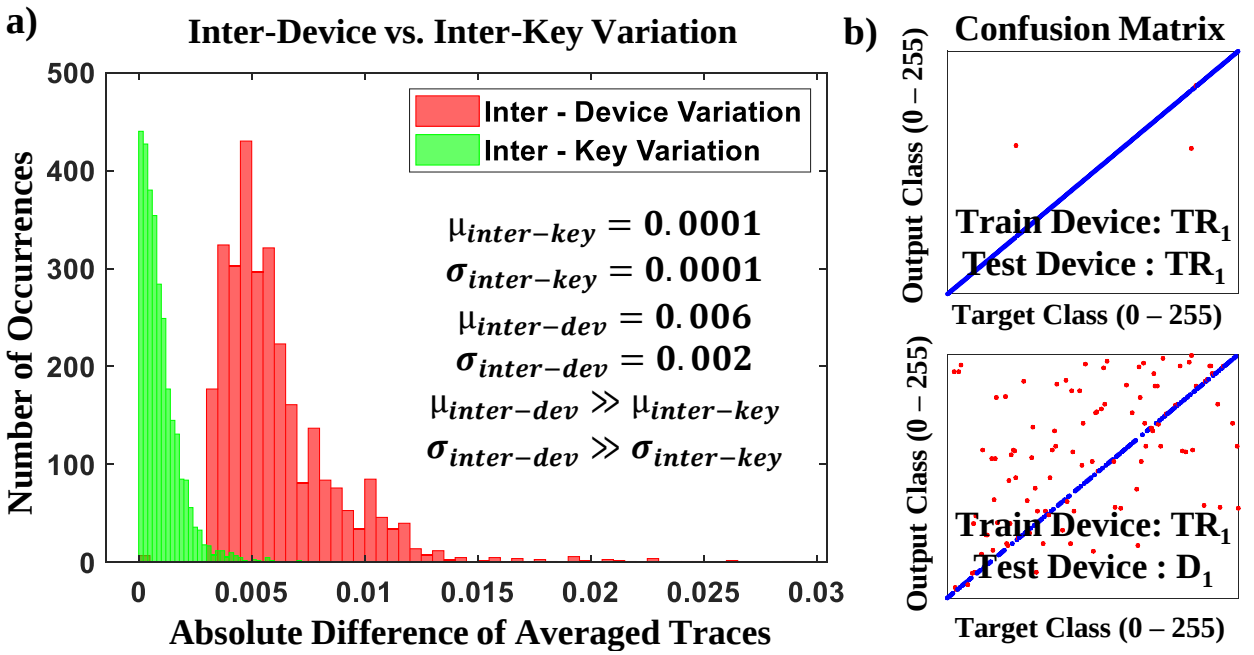


Figure 2.2. (a) Histogram plot showing that the mean of device-to-device variations of the power traces is significantly higher than the mean of key-to-key (class) variations for one device. 40 traces with 3000 time samples each were used in each case. (b) Training with one device (TR_1), the 256-class DNN is able to classify unseen test traces from the same device (TR_1) accurately as seen from the confusion matrix, while it does not generalize for other devices and misclassifies many test traces from a different device (D_1).

- Finally, we show that the `X-DeepSCA` attack performs $> 10\times$ better in terms of MTD, with different signal-to-noise ratio (SNR) scenarios, reducing the time of attack from minutes to seconds (Sec. 5).

2.2 Related Work

Template-based profiling power SCA attacks are extremely powerful as they can potentially break the encryption key within a few encryption traces [61], [73]. Recently, machine learning (ML) based profiling attacks have been studied extensively [64]–[66], [74]–[76]. These ML-based attacks use supervised learning models like the support vector machine (SVM), Self-Organizing Map (SOM) or Random Forest (RF) for classification.

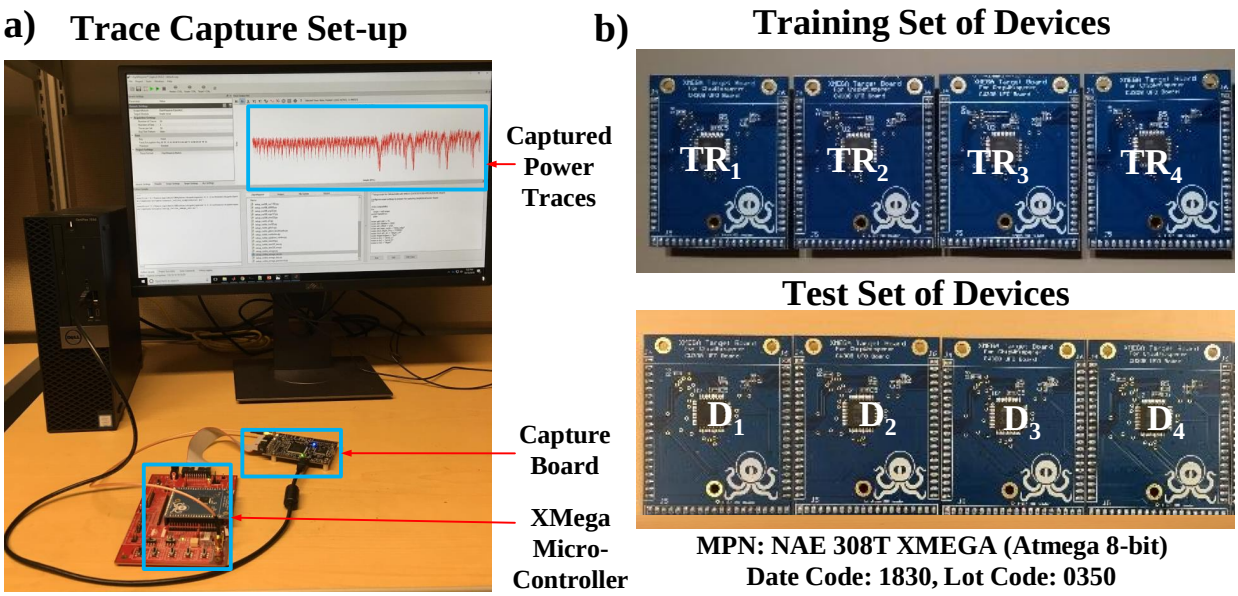


Figure 2.3. (a) Trace Capture Set-up using the Chipwhisperer platform. (b) Traces are captured from multiple Atmega microcontroller devices (TR_{1-4}) for training a DNN so that the model is able to generalize to any other target device (D_{1-4}).

Deep neural networks (DNNs) have generated significant interest in the recent years. It has been shown that the clock-jitter based countermeasures against power/EM SCA can be broken using a convolutional neural network (CNN) [67], [70], [77]. Also, masking based countermeasures have been shown to be broken with neural networks [68], [69].

A summary of the related works is shown in Table 2.1. Most of the existing works [61], [65]–[68], [74]–[76] on profiling attacks have tested their attack on the same device used for the template generation. [73], [78], [79] have evaluated cross-device template-based attacks (TA) using statistical multivariate analysis, Principal Component Analysis (PCA), Mutual Information Analysis (MIA) and Linear Discriminant Analysis (LDA). [80] showed a multi-device profiling using statistical TA.

However, none of the ML-based works have focused on the cross-device attacks yet. Also, the previous works based on neural networks (NNs) have evaluated their models with the same device used for training. We have seen in Figure 2.2(a), the inter-device variation is typically much higher than the inter-key (or inter-class) variations. Hence, a NN model

Table 2.1. Overview of the Related Works on Profiling Attacks

Train/Test Scenario	Profiling SCA Attacks	Classifier
Train and Test with the same Device	[61], [65], [66], [67], [68], [69], [74], [75], [76]	SVM, RF, FCN, CNN, Statistical TA
Train with one device and Test with different Device	[73], [78], [79]	PCA/LDA, MIA, Statistical TA
Training with multiple devices, test with different devices	[80]	Statistical TA
	This Work*	**DNN**

**First Cross-device Deep-Learning Side-Channel Attack*

evaluated against the same device may not necessarily work well on a different target device. This work shows the first cross-device profiling attack using a deep neural network (DNN).

To train a neural network, the typical leakage models used for the power consumption are the Hamming Weight (HW) model (9-class classification), and the identity (ID) model (256-class classification) [70]. In this work, we use the identity model for 256-class classification and train our DNN to learn the leakage information accurately. For all the analyses shown in this work, the attacks are performed on the 1st key byte of the AES-128 encryption engine.

Also, most of the **previous NN models** have been **evaluated on the available DPA v4 contest dataset**, or the newly published ASCAD database [77] which, to the best of our knowledge, **do not contain traces from multiple devices**. Hence, to evaluate our cross-device attack, we built a new database by capturing traces from multiple devices using the Chipwhisperer platform (Figure 6.1(a)). Separate sets of Atmega microcontrollers (Figure 6.1(b)) running AES-128 are used for profiling and testing the `X-DeepSCA` attacks.

2.3 Single Trace `X-DeepSCA` Attack

In this section, we evaluate a single-trace `X-DeepSCA` attack. A 256-class classifier is necessary to perform a single-trace cross-device SCA attack (`X-DeepSCA`). However, designing a 256-class classifier is significantly more difficult compared to the HW-based 9-class classifier.

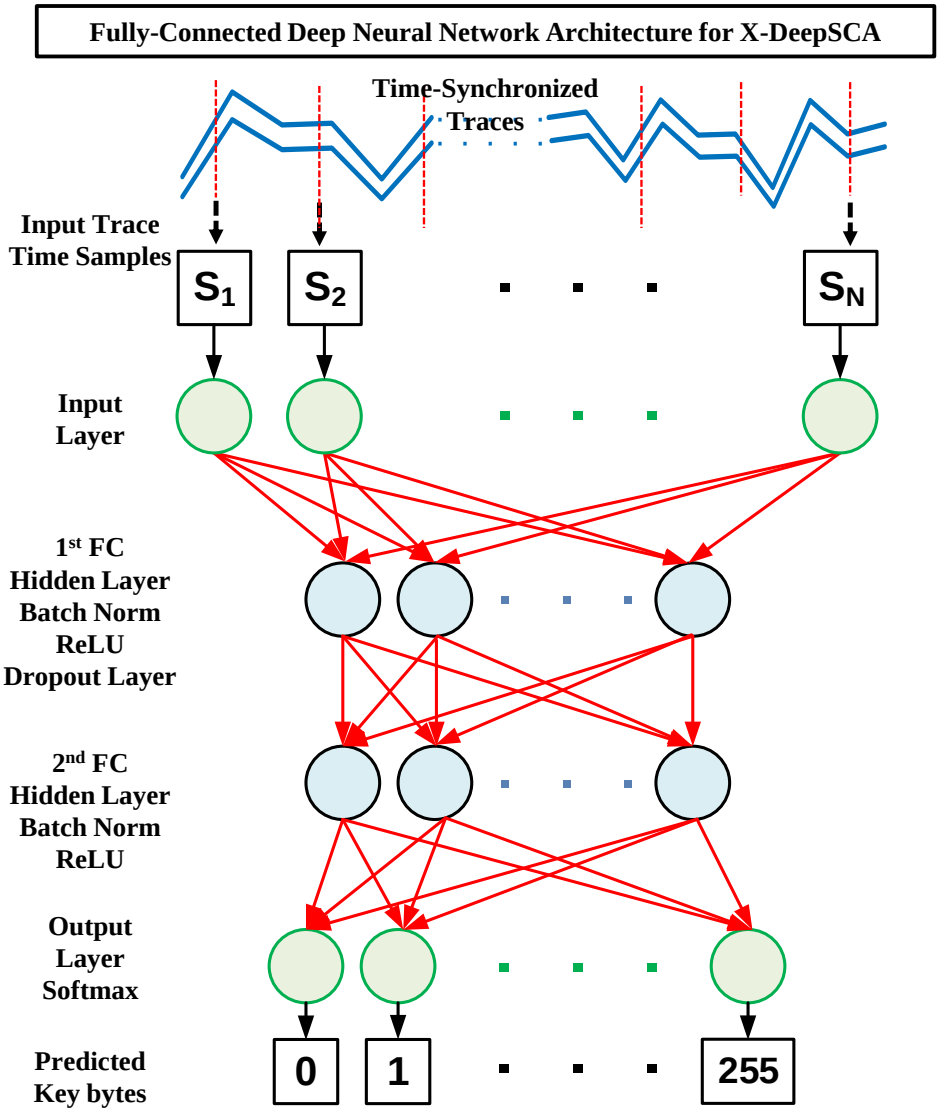


Figure 2.4. Architecture of the proposed Fully Connected DNN for `X-DeepSCA`. The input layer consists of N = 500 neurons. The 1^{st} fully-connected (FC) hidden layer consists of 200 hidden neurons, followed by Batch Normalization, Rectified Linear Unit (ReLU) activation, and a dropout layer. The 2^{nd} hidden layer is similar without the dropout layer. Finally, the output layer has 256 neurons for predicting the correct key byte utilizing the softmax function. If the traces are not aligned in time, a convolutional layer as the input layer would be required. In this work, we use the Fully Connected DNN as the traces captured from the Chipwhisperer are time-aligned.

Hence, choice of the hyperparameters like the learning rate, number of hidden neurons, dropout, are extremely critical to prevent overfitting or underfitting.

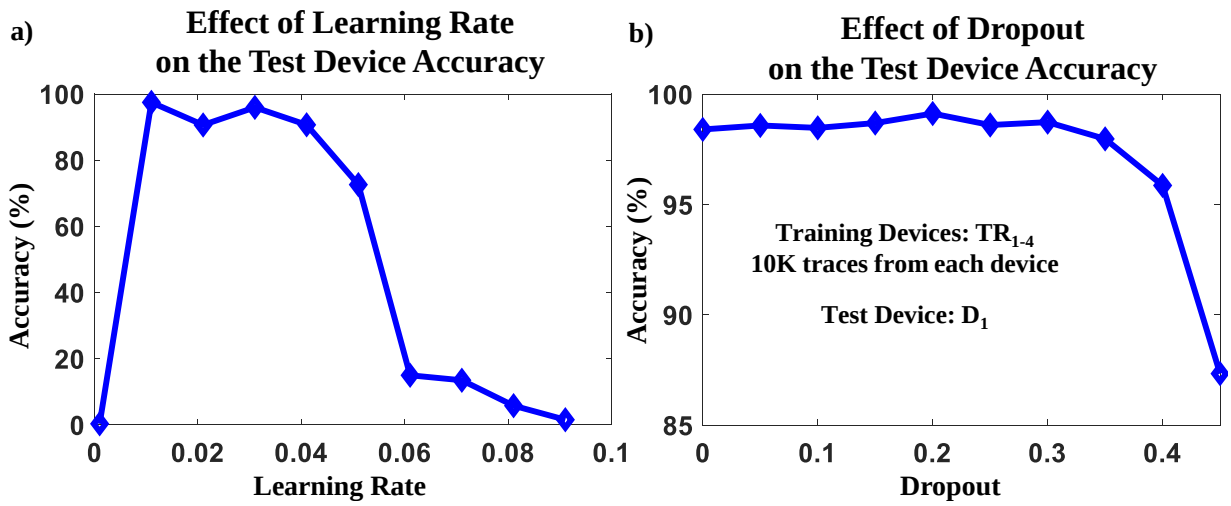


Figure 2.5. Effect of Model Hyper-parameters on the Test Accuracy (on the test device D_1 after training with TR_{1-4}): (a) Learning rate (LR) of ~ 0.01 provides the maximum test accuracy, and higher LR leads to overfitting of the DNN reducing the test accuracy. (b) Lower dropout shows higher accuracy which implies that the data gathered from the microcontroller devices has sufficient electronic noise which helps generalize to unseen data. Dropout higher than 0.3 reduces the accuracy.

2.3.1 DNN Architecture

Figure 2.4 shows the architecture of the proposed fully-connected (FC) DNN for the `X-DeepSCA` attack. Note that, for our work, the traces collected from the Chipwhisperer platform are time-synchronized and hence use of a convolutional layer is not necessary. Although the captured traces from the AES-128 encryption engine (clocked at 7.37 MHz) had 3000 time samples (ADC sampling frequency of 29.48 MHz) for an entire encryption operation, it was initially fed to the DNN and verified that the network learns accurately from the points of leakage (cross-verified using a CPA attack) within the first 200 time samples for the 1st key byte under attack. After this verification[1], to reduce the model complexity (and the time for training the DNN), only the first 500 time samples from each power trace were fed to the DNN.

[1]↑It is also worth noting that the DNN model can also serve as a leakage assessment tool for cryptographic devices.

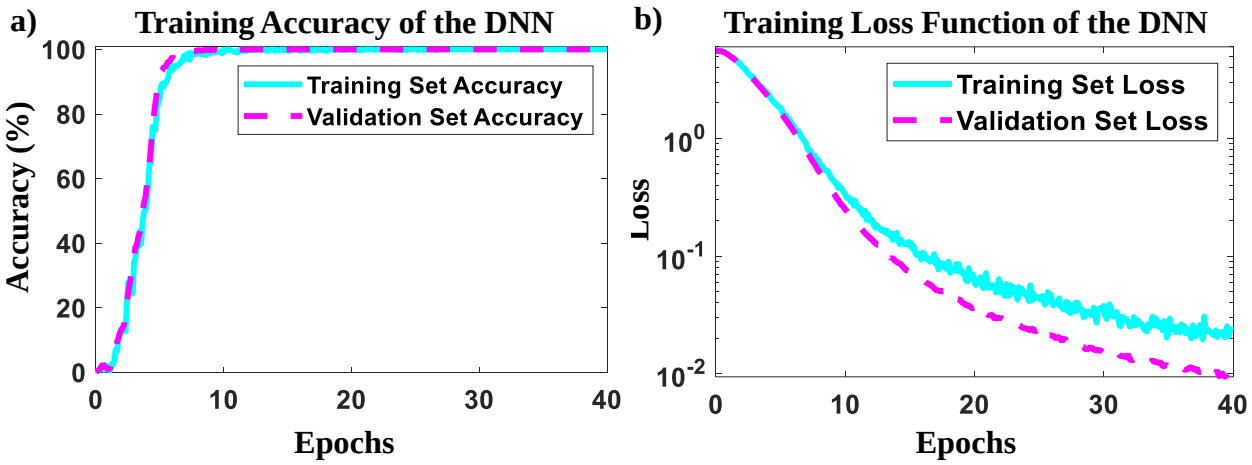


Figure 2.6. (a) Training and Validation Accuracy of the DNN reaches $\sim 100\%$ within 25 epochs and does not show any overfitting. (b) Loss function of the DNN for both the training/validation sets. Note that training and validation have been performed with data from all the 4 devices (TR_{1-4}).

The first FC layer of the DNN consists of 200 neurons, and increasing the number of hidden neurons may lead to overfitting. Batch normalization layer [81] and the dropout layers provide regularization to prevent overfitting and encourage generalization to unseen data. The Rectified Linear Unit (ReLU) is used as the non-linear activation function to learn non-linear mappings from the input to the output. The second FC layer is similar without the dropout layer, and is finally followed by the output layer with 256 neurons, which predicts the correct key byte in a single trace utilizing the softmax function. The loss function used was categorical cross-entropy, optimized with the Adam algorithm and with a batch size of 32.

Figure 2.5(a, b) shows the effect of some of the hyper-parameters of the DNN model on the accuracy of a different test device. Figure 2.5(a) shows that a learning rate of 0.01 provides the maximum test accuracy, while a higher learning rate could lead to overfitting resulting in reduced test device accuracy. From Figure 2.5(b), we see that even in case of low dropout, the test accuracy remains high, which implies that the data gathered from the *real-world devices has sufficient electronic noise*. However, dropout more than 30% leads to reduced classification accuracy.

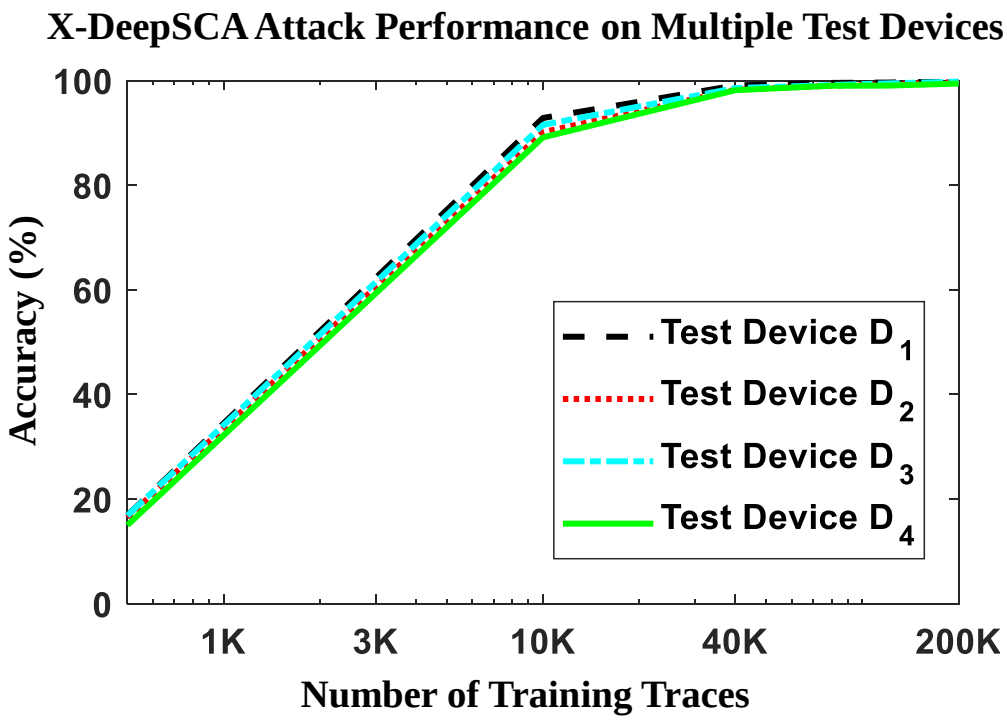


Figure 2.7. Attack Accuracy on the test devices (D_{1-4}) with the DNN model trained with varying number of training traces gathered from the 4 training devices, where each of them (TR_{1-4}) contributed equally .

To train the DNN, for all our experiments (unless otherwise mentioned), 10K traces (equally distributed for all the 256 possible values for the 1^{st} key byte (classes) with a fixed plaintext) from each of the four devices were augmented together, and 20% of the total number of traces were kept for validation of the DNN during the profiling phase.

2.3.2 Performance Analysis of Single-Trace `X-DeepSCA` Attack

Figure 2.6(a,b) shows the training and validation accuracies of the DNN. We can see that the DNN model reaches an accuracy of $> 99.9\%$ within 25 epochs and also that the training and validation loss approach 0. The validation set accuracy remains almost same as that of the training set, implying that the DNN model is not overfitting. Note that the validation loss is lower since the dropout layer is present during training and not for the validation.

Figure 2.7 shows the performance of the trained DNN model on the test devices (D_{1-4}) with varying number of training traces, drawn equally from all the four devices (TR_{1-4})

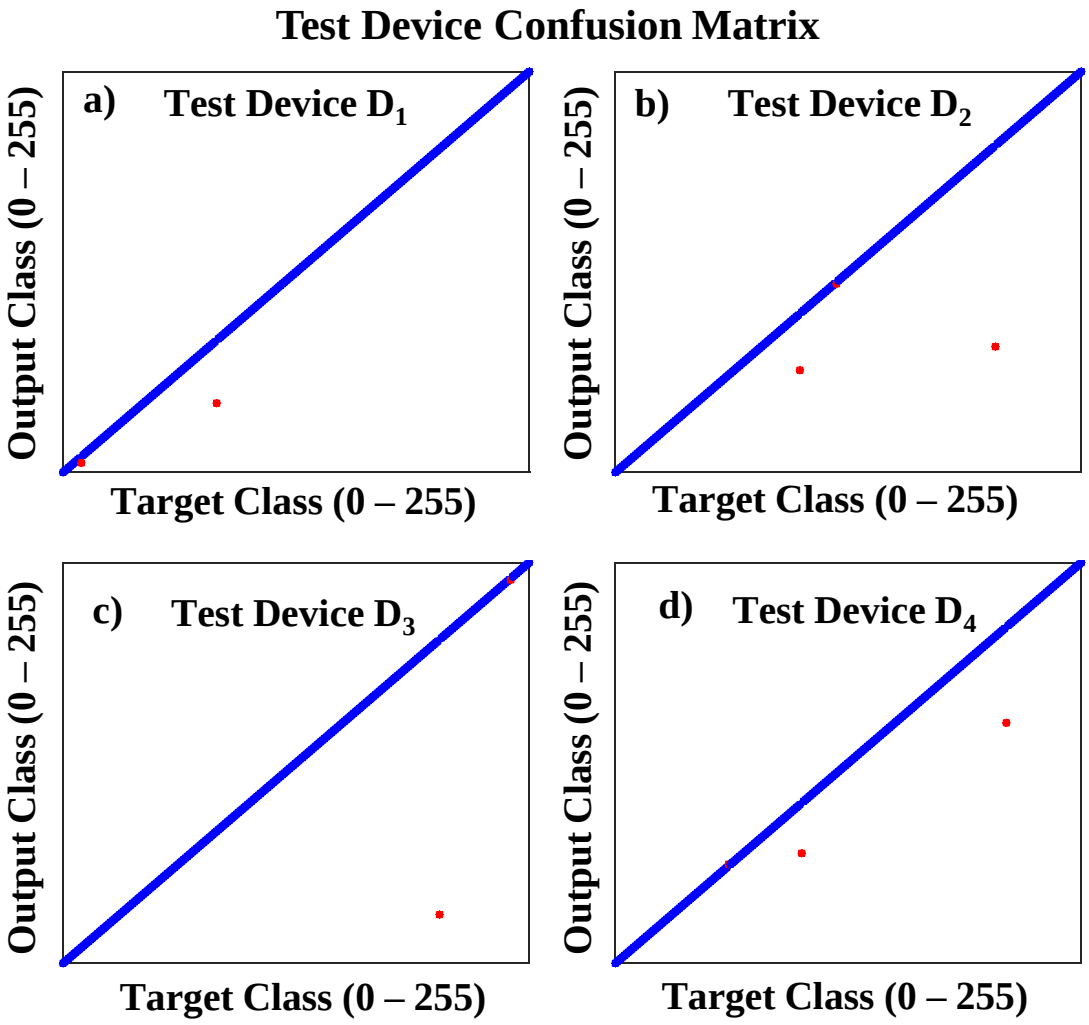


Figure 2.8. Confusion matrix for each of the test devices (D_{1-4}). At most 3 key bytes out of the 256 ($\sim$ 99% overall accuracy) are getting misclassified for each of the test devices, with the DNN model trained with 10K traces from each of the 4 training devices (TR_{1-4}).

reserved for training. The `X-DeepSCA` attack on all the 4 test devices shown reaches 99% accuracy with 40K training traces, and $>$ 99.9% with 200K training traces in total(drawn equally from each of TR_{1-4}).

Note that for the test devices, traces are collected for different keys to evaluate the accuracy of all the classes (key bytes). Figure 2.8(a-d) shows the confusion plots on the test devices (D_{1-4}) after training with 40K traces (10K from each of the 4 training devices). As

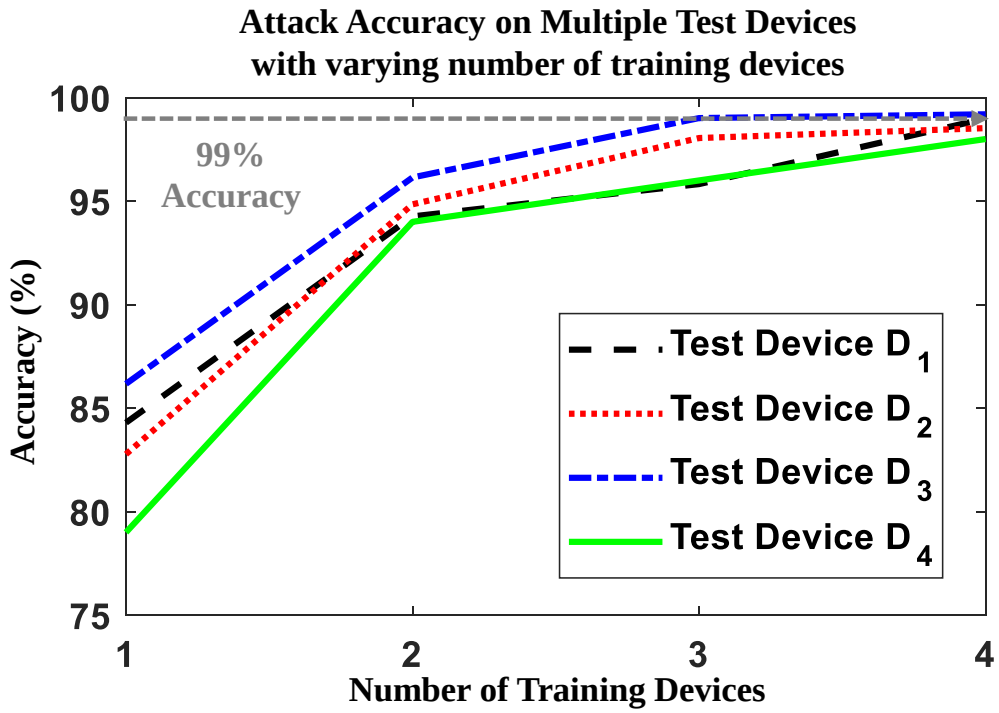


Figure 2.9. Effect of augmenting traces from Multiple Devices during training: As the number of devices is increased, the DNN model generalizes well to new devices (D_{1-4}) and hence the accuracy improves and reaches 99% with 4 training devices (TR_{1-4} - 10K traces each).

expected, for all the test devices, we see that at most 3 key bytes are misclassified (marked in red, outside the diagonal line) out of the all 256 different key bytes.

Figure 2.9 shows the effect of augmenting traces from multiple devices (with 10K traces each) for training the DNN. We see that with only 1 training device, the accuracy on a test device goes to $\sim$ 80%, while it increases to $\sim$ 99% after augmenting traces from all the 4 training devices with only 10K traces captured from each device.

2.4 N-Trace `X-DeepSCA` Attack

In the previous section, we have shown that a single-trace `X-DeepSCA` attack with an accuracy of $>$ 99.9% (averaged over all the 256 classes) can be performed on a test device, with 200K training traces (equally from each of the devices TR_{1-4}) used to build the DNN

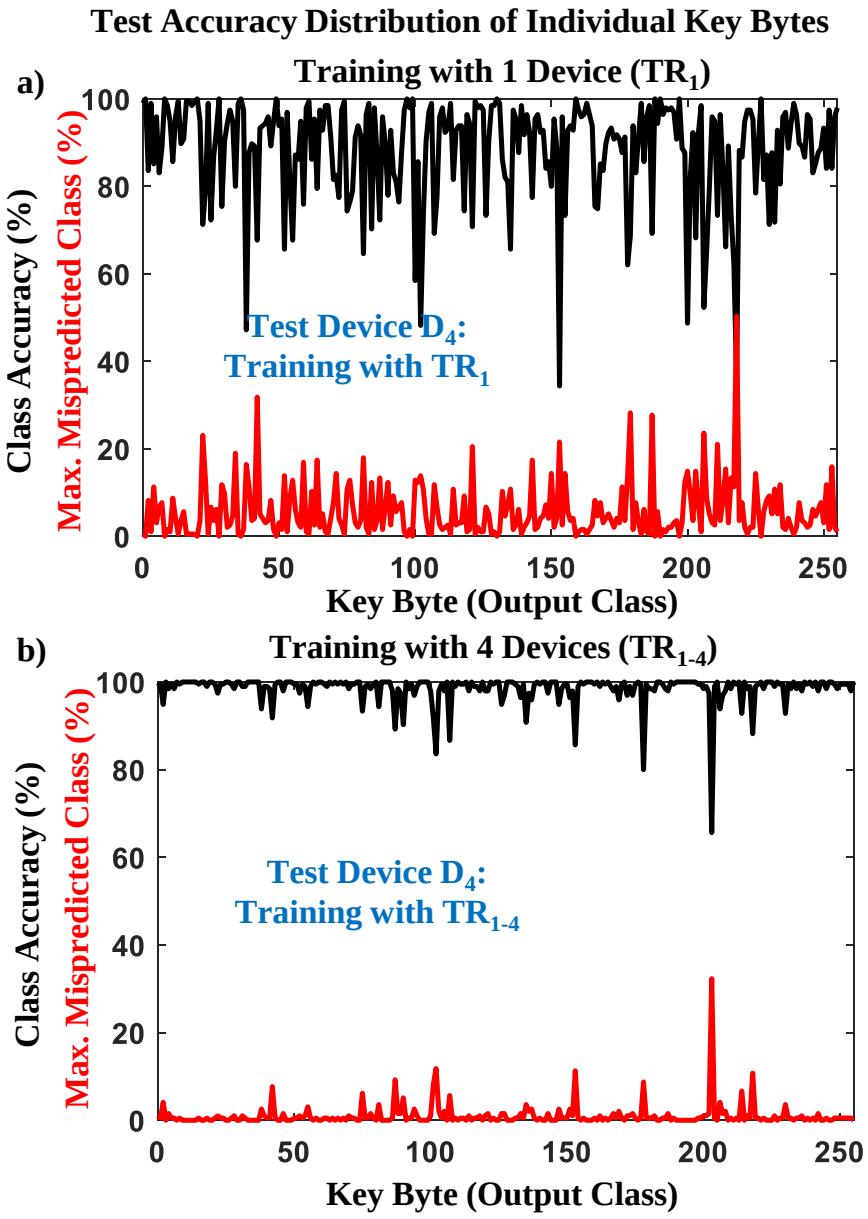


Figure 2.10. Individual Key Byte (Class) Accuracy Distribution for the test device D_4 (showed the worst average accuracy out of the D_{1-4}): The black plot represents the accuracy for each key byte, and the red plot denotes the maximum percentage of a particular class misprediction for the test device D_4. (a) With 1-device training (TR_1 - 10K traces), for some of the key bytes the black and red curves overlap, while (b) with 4-device (TR_{1-4} - 10K traces each) training, there is a significant reduction in the measure of entropy and an N-trace attack would be able to predict even the lowest accuracy key byte with high success probability (refer to Fig. 2.11).

model. In this section, we analyze the individual class (key byte) accuracies to evaluate the practicality of a single-trace attack.

2.4.1 Individual Key Byte Accuracy

Figure 2.10(a, b) shows the individual key byte (class) accuracies and the percentage of the misclassified key byte with the highest occurrence in prediction (for every key byte class) for the test device D_4 (as it showed the lowest accuracy of the 4 test devices and poses the worst case scenario for an attacker). The separation between the class accuracy ($K_{pred} = K_{target}$) and the maximum percentage of the mispredicted class (the particular key byte which is wrongly predicted maximum number of times - $K_x \neq K_{target}$) gives a measure of the entropy ($\eta_{K_{target}}$) of the `X-DeepSCA` attack, as shown in Eqn. 1,

$$\eta_{K_{target}} = 1 - \left[\frac{|K_{pred} = K_{target}|}{|K_{total}|} - \frac{argmax(|K_{pred} = K_x| : K_x \neq K_{target})}{|K_{total}|} \right] \tag{2.1}$$

where, K_{pred} represents the predicted key byte, K_{target} is the target key byte, K_x is any other key byte (mispredicted) which has the maximum occurrence for the K_{target} class, and $|K_{total}|$ denotes the total number of queries (traces) for that particular K_{target} class.

Figure 2.10 shows that training with 4 devices has significantly lower entropy ($\eta_{K_{target}}$) compared to 1-device training. Also, we see from Figure 2.10 that although the test device D_4 achieves an average accuracy of $> 99\%$ (most of the key bytes can be broken with a single-trace), as seen from Figure 2.7, 2.9, the minimum accuracy of few key byte drops below 80%. Hence, although the single-trace attack will succeed on most key bytes, it may not work for a few key bytes, and a multi-trace attack is required.

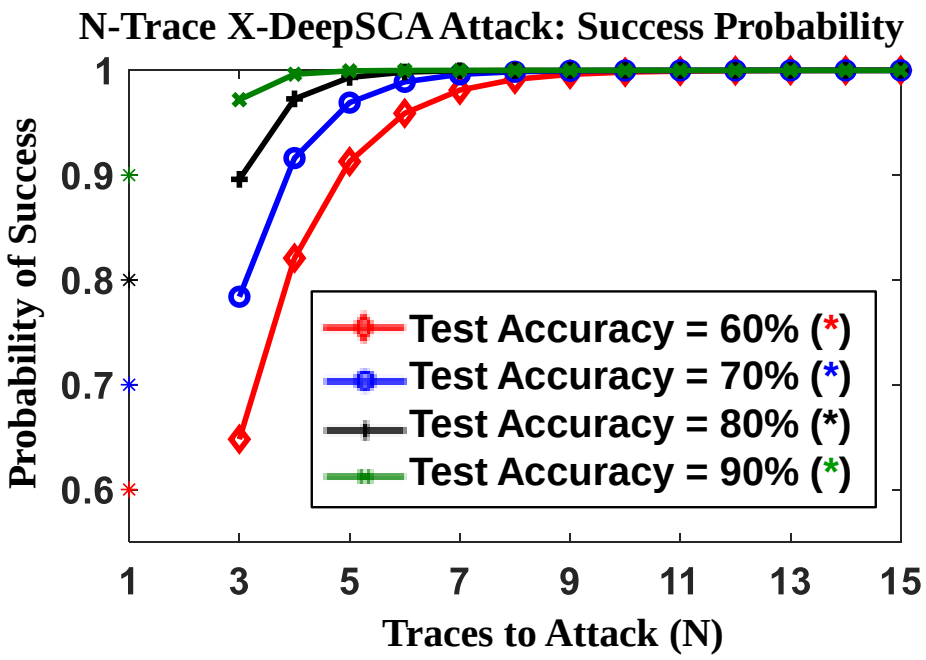


Figure 2.11. N-trace `X-DeepSCA` Attack: Number of traces required by an attacker to achieve a confidence of 99.9%. Even for classes with low accuracies, the N-trace `X-DeepSCA` attack would reveal the correct key byte within $N \leq 10$ traces, as long as the individual class accuracy remains higher than the % of maximum mispredicted key byte for that class.

2.4.2 Success Probability of the N-trace `X-DeepSCA` attack

Using the concept of majority voting, we propose an N-trace `X-DeepSCA` attack. The number of encryption traces required to gather in order to achieve a confidence (probability of success) of 99.9% can be mathematically derived, as shown in Eqn. 2 (valid for $N \geq 3$):

$$\begin{aligned} Pr(Maj(N) = K_{target}) &= \sum_{x=2}^{N} Pr(x) \\ &= \sum_{x=2}^{N} \binom{N}{x} p^x (1-p)^{N-x} \frac{^{255}P_{N-x}}{255^{N-x}} \end{aligned} \tag{2.2}$$

where, $Pr(Maj(N) = K_{target})$ gives the probability of a successful target key recovery using the majority voting with N traces, p is the single-trace test accuracies for each class (key byte value), P represents the permutation operator. Note that the underlying assumption of Eqn. 2 is that the class accuracy and the class misprediction distributions are uniform, and

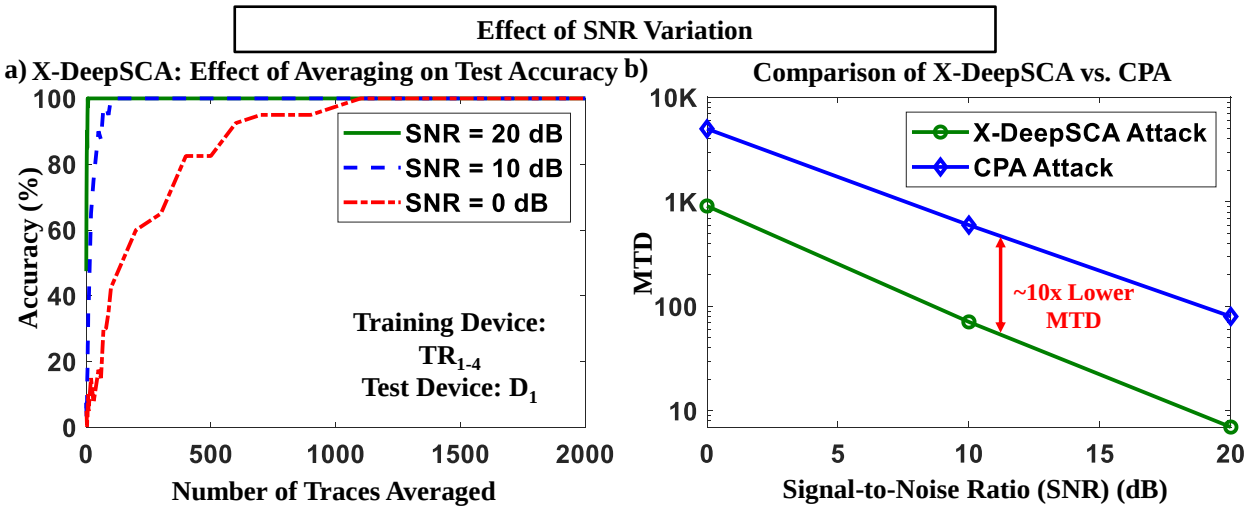


Figure 2.12. (a) Number of traces (averaged) required for a successful `X-DeepSCA` attack (with $>$ 99.9% accuracy) in different SNR scenarios. For SNR=20dB, averaging with less than 10 traces is sufficient to achieve $>$ 99.9% accuracy, while it requires $\sim$ 100 traces for SNR=10dB, and $\sim$ 1000 traces for SNR=0 dB to be averaged over to achieve the 99.9% accuracy. (b) Comparison of the `X-DeepSCA` attack with traditional CPA attack shows a lower MTD for `X-DeepSCA` for all SNRs.

there is no overlap between them for any of the individual key bytes. Hence, as seen from Figure 2.10(b), majority voting works as the entropy is reduced, and even for the lowest accuracy key byte (with 70% accuracy, $p = 0.7$), N-trace `X-DeepSCA` attack achieves an accuracy (success probability) of 99.9% with $N \leq 10$ encryptions, as shown in Figure 2.11 (derived from Eqn. 2).

2.5 Discussions

2.5.1 `X-DeepSCA` Attack: Effect of SNR Variation

Now, we evaluate the effect of varying Signal-to-Noise Ratio (SNR) on the efficacy of the `X-DeepSCA` attack. Figure 2.12(a) shows the number of traces required to average for a successful `X-DeepSCA` attack with $>$ 99.9% accuracy on the test device D_1 using the training set with TR_{1-4} (10K traces each). Figure 2.12(b) shows that the number of traces required to retrieve the correct key byte of the AES-128 engine under attack is $\sim 10\times$ lower than the

traditional CPA attack (at the 1^{st} round S-box output using Hamming Weight(HW) leakage model) for different levels of SNR.

2.5.2 Future Work

For the future scope of this work, the efficacy of the proposed `X-DeepSCA` attacks can be further improved if we can guarantee that the accuracy of each key byte and the mispredicted classes for that key byte are uniformly distributed. This could be achieved by ensuring that the DNN has minimum bias during a misclassification, which would lower the number of traces (N) required for a successful N-trace `X-DeepSCA` attack. Overall, the proposed attack can put a huge dent to the security of embedded devices.

2.6 Conclusions

For the first time, this work shows a Cross-device Deep Learning based Side-Channel Analysis (`X-DeepSCA`) attack. Utilizing multiple (4) devices for training a fully-connected DNN, results showed that an average accuracy of 99.9% can be achieved with all the 4 test devices using 200K training traces, showing the possibility of a single-trace attack. However, deeper analysis utilizing the proposed measure of entropy revealed that few individual key bytes had lower accuracies, and hence an N-trace `X-DeepSCA` attack ($N \leq 10$) is proposed to break the key with $> 99.9\%$ confidence. Finally, we show that for varying SNR scenarios, the proposed `X-DeepSCA` attack achieves $\sim 10\times$ lower MTD, which breaks the target devices within seconds compared to a few minutes for the traditional CPA attack, increasing the threat surface significantly.

In the next chapter, we will look into the white-box analysis of the EM SCA leakage from a crypto IC to develop an energy-efficient countermeasure against both power as well as EM SCA attacks.

3. STELLAR: EM SIDE-CHANNEL ATTACK PROTECTION THROUGH GROUND-UP ROOT-CAUSE ANALYSIS

Most of the materials in this chapter have been extracted verbatim from the paper:
1. Debayan Das, Mayukh Nath, Baibhab Chatterjee, Santosh Ghosh, Shreyas Sen, STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2019.

The threat of side-channels is becoming increasingly prominent for resource-constrained internet-connected devices. While numerous power side-channel countermeasures have been proposed, a promising approach to protect the non-invasive electromagnetic side-channel attacks has been relatively scarce. Today's availability of high-resolution electromagnetic (EM) probes mandates the need for a low-overhead solution to protect EM side-channel analysis (SCA) attacks. This work, for the first time, performs a white-box analysis to root-cause the origin of the EM leakage from an integrated circuit. System-level EM simulations with Intel 32 nm CMOS technology interconnect stack, as an example, reveals that the EM leakage from metals above layer 8 can be detected by an external non-invasive attacker with the commercially available state-of-the-art EM probes. Equipped with this 'white-box' understanding, this work proposes *STELLAR*: Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing, which is a two-stage solution to eliminate the critical signal radiation from the higher-level metal layers. Firstly, we propose routing the entire cryptographic core within the local lower-level metal layers, whose leakage cannot be picked up by an external attacker. Then, the entire crypto IP is embedded within a Signature Attenuation Hardware (SAH) which in turn suppresses the critical encryption signature before it routes the current signature to the highly radiating top-level metal layers. System-level implementation of the STELLAR hardware with local lower-level metal routing in TSMC 65 nm CMOS technology, with an AES-128 encryption engine (as an example cryptographic block) operating at 40 MHz, shows that the system remains secure against EM SCA attack even after $1M$ encryptions, with 67% energy efficiency and 1.23× area overhead compared to the unprotected AES.

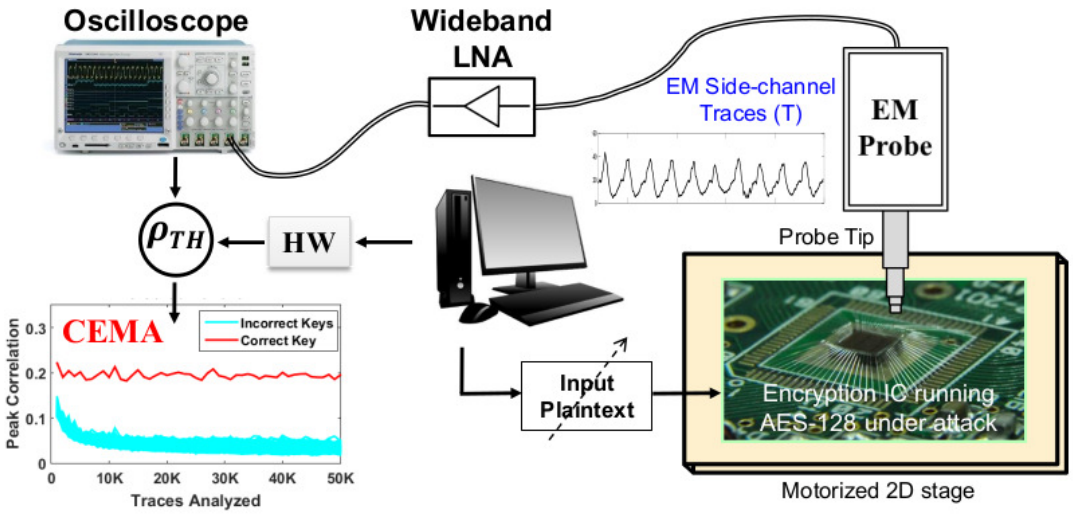


Figure 3.1. EM Side-Channel attack Overview.

3.1 Background

3.1.1 Preliminaries

The EM analysis attack is a prominent non-invasive side-channel attack (SCA) on cryptographic ICs and has been demonstrated over the last decade [32], [82]. The EM analysis attack is typically performed in two phases. In the first phase, the attacker collects the EM emanations using an EM probe optionally connected to a low-noise amplifier (LNA) placed in the vicinity of the encryption device under attack. In the second phase, the collected EM traces are subjected to simple (SEMA) or differential EM analysis (DEMA) [83] to extract the secret key of the encryption device.

Figure 3.1 shows how a EM side-channel attack is performed. Initially, the EM emanations of the device performing encryption is measured in an oscilloscope or a high-resolution analog-to-digital converter (ADC), and the EM traces (T) are collected over varying input plain-texts for the same secret key. Next, for a correlational EM analysis (CEMA) [84], a hypothetical EM leakage model like the Hamming distance matrix (H) is built which contains the expected EM leakage of the device performing a particular operation during encryption (like the S-box operation in the first round of AES), over the given plain-texts

with all possible key bytes. This reduces the key search space of the AES-128 to 2^8=256 possibilities for each byte of the secret key. Finally the correlation co-efficient (ρ_{TH}) between the EM hypothesis (H) and the obtained traces (T) is calculated over time. One significant advantage of CEMA (or, CPA for power analysis) is that the precise knowledge of the time instance when the targeted operation occurs is not required, since ρ_{TH} can be calculated at each sampling point of the trace. The key byte showing the maximum correlation represents the correct key byte. Repeating the process 16 times reveals the entire 128 bits of the secret key.

Real-world examples of EM SCA include the counterfeiting of e-cigarette batteries by stealing the secret encryption keys from the authentic batteries to gain market share. In general, electromagnetic analysis attacks can be used to extract the hidden key from the boot-loader of any embedded VLSI device [32], [82], [85].

3.1.2 Motivation

Power and EM SCA attacks on encryption ICs have gained tremendous importance over the last decade [86], [87], [85], [88]. Although researchers have mainly focused on countermeasures against power SCA, preventing EM attacks is gaining more prominence in the present era of IoT, due to the availability of commercial inexpensive EM probes. Being in the close proximity of the encryption device, the EM side-channel leakage can be captured non-invasively using low-cost EM probes, in contrast to the requirement for physical probing in power analysis attacks. Hence, a low-overhead generic countermeasure that can be commonly utilized for both power and EM side-channel resilience is extremely necessary.

This work performs a ground-up analysis to root-cause the origin of the EM leakage in an integrated circuit (IC). After identifying the source of the EM leakage, we investigate the existing state-of-the-art power and EM SCA countermeasures that can be utilized for protecting the cryptographic IC. Among the existing countermeasures, the recently proposed Attenuated Signature Noise Injection (ASNI) [42] is a generic and low-overhead solution to protect against power SCA. In this work, we propose ***STELLAR*: Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing**, utilizing Signature Attenuating

Hardware (SAH) to embed the entire cryptographic IP of an electronic system with local low-level metal routing and thereby significantly attenuate the signature before it reaches the top metal layers of the chip, which leaks critical information through EM side-channels.

In this article, as an application of the proposed countermeasure, we focus on a 128-bit AES engine. Correlational EM analysis (CEMA) with Hamming distance (HD) model [84] is employed for the attack.

3.1.3 Contribution

Specific contributions of this chapter are:

- This work, for the first time, performs a ground-up root-cause analysis to develop the fundamental understanding, i.e. a 'white-box model' of the *key source of EM information leakage* from the current path of a cryptographic IC. System-level simulations using Ansoft HFSS for 32 nm Intel CMOS technology, as an example, reveals that EM leakage is detectable using state-of-the-art commercial probes from metal layers only higher than 8.

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

- In order to suppress the AES encryption (or the whole cryptographic core in general) signature, STELLAR utilizes a Signature Attenuating Hardware (SAH), such as Attenuated Signature Noise Injection (ASNI) [42], to attenuate the correlated AES current

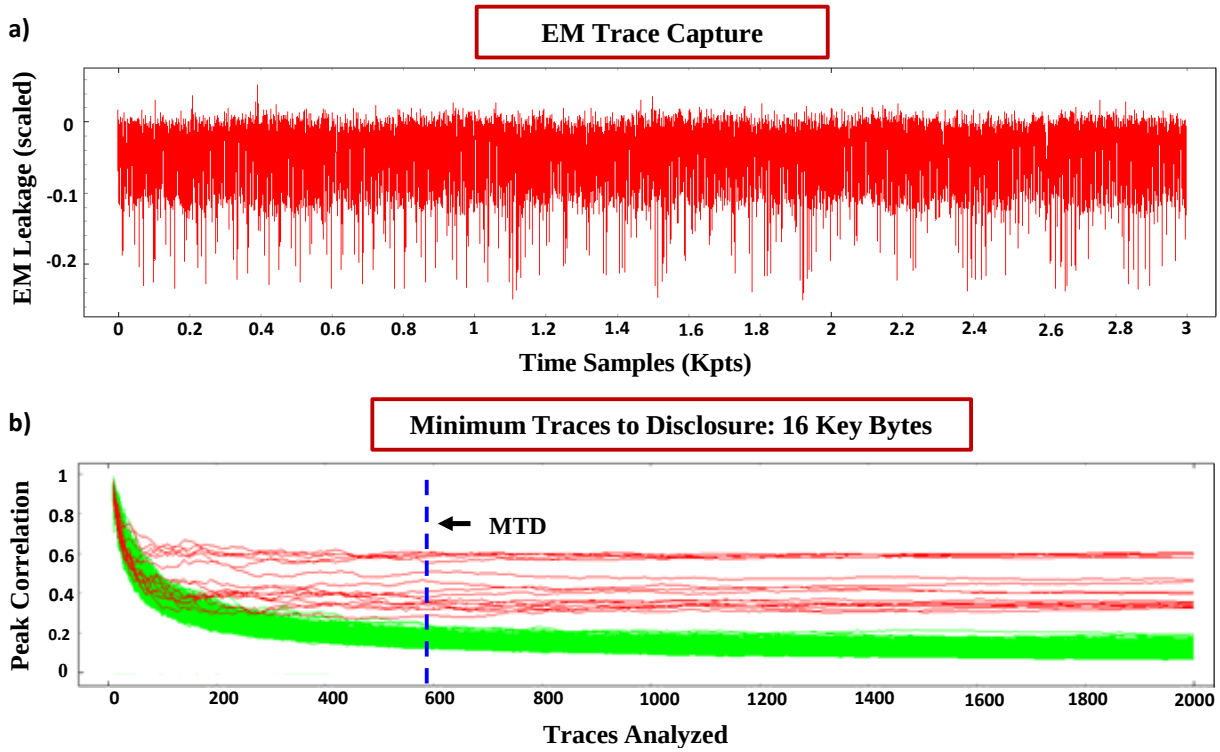


Figure 3.2. Correlation EM Side-channel attack on the Atmega microcontroller running AES-128. (a) The EM traces gathered from the oscilloscope, (b) CEMA attack on the unprotected AES core shows $MTD < 600$ traces.

signature significantly before it reaches the higher metal layers, thereby enabling EM as well as power SCA immunity.

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

3.2 Related Work

Our EM SCA attack set-up involves a target Atmega microcontroller (using the Chipwhisperer platform) [89] running AES-128 encryption, and the EM field is picked up by a nearby EM probe connected to a low-noise amplifier (LNA) and captured using an oscillo-

scope. The oscilloscope data is then downloaded to a PC wherein the correlation EM analysis (CEMA) is performed to reveal each byte of the secret key. As seen from Figure 3.2(a, b), all the 16 key bytes of the AES-128 implementation can be obtained within < 600 traces, thereby breaking the security of this system. Although this is a basic example to prove the feasibility of EM SCA, it demonstrates the potency of EM SCA attacks on electronic systems.

3.2.1 Literature Review: Black Box Approach

Several EM side-channel attacks have been demonstrated over the last few years. In CHES 2002 [90], it was first shown that the EM spectrum could be sensed to perform SCA. There have been few works to scan the EM emissions of integrated circuits in time-domain [91]. Lomne et al. [92] proposed a modeling of magnetic emissions from ICs using Redhawk. Recently, Kumar et al. [93] proposed an efficient simulation set-up to perform EM SCA. However, most of these works focus on top-down modeling of EM emissions from a chip and consider the cryptographic IC as a black box. In CHES 2014 [94], the authors developed an on-chip sensor to detect an approaching probe. In addition, the development of highly sensitive EM probes [32] calls for a fundamental understanding of the characteristics of EM side-channel leakage from cryptographic ICs and trace the critical information-leakage sources in the current path.

Specific countermeasures proposed against EM SCA include signal strength reduction techniques like shielding or signal information reduction using noise insertion [90]. However, data randomization with noise injection comes with significant power overheads, and EM shielding incurs high cost of packaging [95] and is not a practical solution for most applications. To the best of the authors' knowledge, none of these works have thoroughly investigated the root-cause of the EM leakage in a cryptographic IC.

3.2.2 Genesis of the EM Leakage: A White box Approach

Although the source of leakage in the case of power analysis attack is well understood and analyzed [86], [96], [41], the origin of EM leakage in the context of side-channel security

is still not well-perceived. In this work, we conceive a ground-up approach to analyze and root-cause the genesis of this EM side-channel leakage in a CMOS IC.

For an integrated CMOS-based circuit, in steady-state, there is no static current flowing through the circuit. However, the presence of stationary charges in the circuit give rise to electric fields ($\vec{E}$), as can be explained from Gauss' Law ($\nabla \cdot \vec{E} = \frac{\rho}{\epsilon}$). As the output of logic gates switches its state, moving charges (dynamic and leakage currents) create changing electric fields, which in turn produce magnetic fields (known as modified Ampere's law: $\nabla \times \vec{H} = \vec{J} + \epsilon \frac{\partial \vec{E}}{\partial t}$). On the other hand, changing currents (acceleration of charges) produce time-changing magnetic flux, thereby inducing an electric field, which is known as the Faraday's law ($\nabla \times \vec{E} = -\mu \frac{\partial \vec{H}}{\partial t}$). Note that $\vec{E}$ represents the electric field in V/m, $\vec{H}$ denotes the magnetic field intensity in A/m, $\vec{B}$ represents the magnetic field intensity in Tesla (T), $\vec{J}$ is the electric current density in A/m^2, ρ denotes the electric charge density in C/m^3, ϵ is the electric permittivity and μ is the magnetic permeability of the medium.

The present day CMOS architecture consists of a cell-level transistor layer over a silicon substrate, and multiple layers of metal consisting of interconnects and vias [97]. Depending on different CMOS technologies, the number of total metal layers may vary. However, having more number of metal layers is important for integrated circuit design as it not only makes it easier for the circuit designer, but also reduces the area of the chip significantly as the layers are stacked on top of another. The highest metal layers available for a process are used as the power grid. Hence, any signal in the lower-level metal layers has to be routed to the topmost metal layer and through to the copper (Cu) bump, as shown in Figure 3.3(b).

As a result, any cell-level excitation is reflected as a time-varying current through the metal layer routings. The interconnects in the routing, due to the presence of this time-varying current, start functioning as antennas, and emit electromagnetic radiation. Now, the typical operating frequency (f) of industrial digital CMOS circuits lie in the 1-10 GHz range, which corresponds to a wavelength ($\lambda = \frac{v}{f}$, v denotes the speed of propagation of the EM waves and is equal to $3 * 10^8 m/sec$), which is in the order of 30-300 mm, whereas the dimensions of the interconnects are usually three orders of magnitude lower, in the range of few micrometers. This type of excitation structure, where the length of the interconnects is much lower than the wavelength ($l \ll \lambda$), is analogous to infinitesimal dipoles in

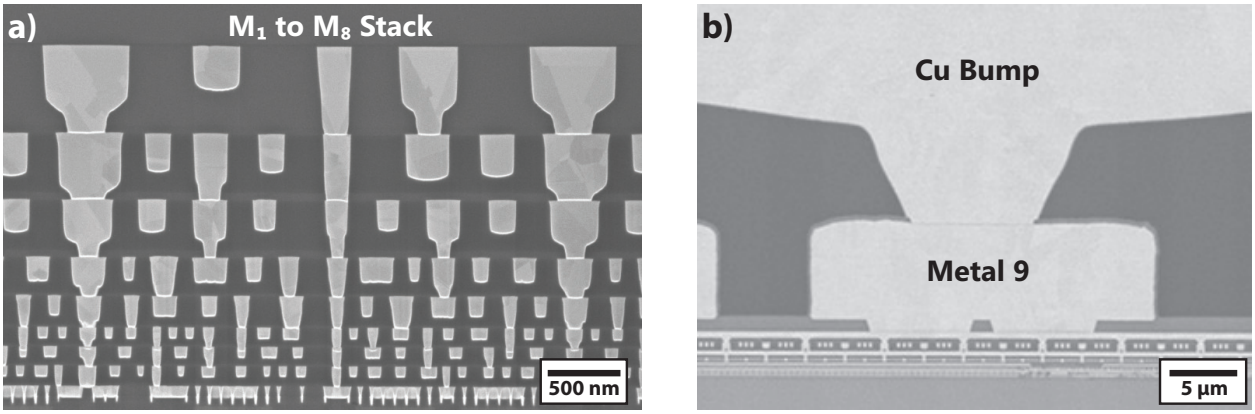


Figure 3.3. Cross-Section of the Interconnect Stack (Intel 32 nm) [97], (a) Metal 1 through 8 (b) Includes metal 9 and the copper bump layer.

antenna theory [98]. For an infinitesimal dipole, the excitation frequency lies far away from the resonant frequency of the antenna, and hence the structure can be analyzed assuming a uniform current amplitude I_0 throughout its length. This is unlike a traditional half wavelength ($\lambda/2$) dipole antenna, where the excitation frequency matches the antenna resonance, and the current distribution forms nodes and anti-nodes along the length of the antenna. Now, as the current distribution in an infinitesimal dipole is uniform, it can be intuitively broken down into unit elements, wherein each element contributes equally (E_{i}) towards the net radiated electric field amplitude E_{rad}. If N is the number of elements, $E_{rad} = NE_{\mathrm{i}}$, and as a matter of fact, N is proportional to the dimensions of the radiation structure. As a result, the radiated field amplitude should have a linear dependence on the dimensions of the structure, e.g. if the length of the structure is l, $N \propto l$ and $E_{rad} \propto N$, so $E_{rad} \propto l$.The radiated power P_{rad} would then be proportional to l^2. In fact, for infinitesimal dipoles, the radiated power can be shown to be proportional to $(l/\lambda)^2$, as given by Eqn. 3.1 [98],

$$P_{rad} = \eta \left(\frac{\pi}{3}\right) \left|\frac{I_0 l}{\lambda}\right|^2 \tag{3.1}$$

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

Thus in essence, the time-varying electric and magnetic fields produce an EM wave during the switching activity of the logic and sequential circuits within an ASIC. A nearby attacker can pick up the radiated "side-channel" EM emissions and extract the secret key from the

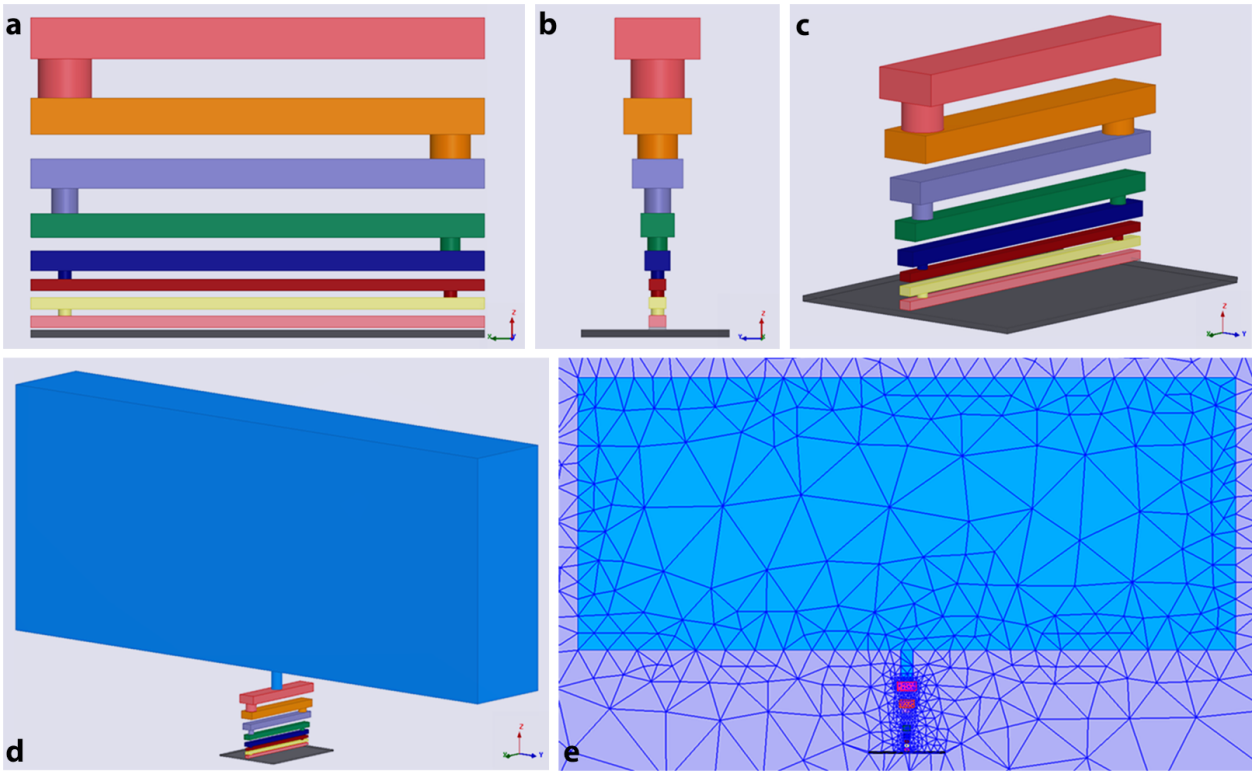


Figure 3.4. Modeling the Interconnect Stack for the Intel 32 nm CMOS process: (a) Metal 1-8 side view, (b) cross-sectional view, and (c) isometric projection; (d) isometric projection with metal layer 9 included; (e) adaptive meshing in HFSS.

encryption engine using CEMA/DEMA. It is therefore essential to understand the origin and exact nature of the radiation from the metal layers in a chip to devise a design strategy in order to counter EM SCA. Also, the magnitude of the EM fields depends on the amount of current flowing in the circuit and the dimensions of the metal layer routings. In the next section, we discuss the modeling of the interconnect stack to analyze the effect of metal layer dimensions on the EM radiation signature.

3.3 Modeling E-Field Emanation from Metal Layers in Modern CMOS Process

As discussed in the previous section, the EM radiation from a CMOS IC primarily originates from the metal layer routings. To develop a better understanding of the situation, the net radiation can be split into contributions originating from each individual interconnect

Table 3.1. Pitch and thickness of metal layers at Intel's 32 nm node [97]

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

in the routing. A simple structure that can be used to analyze the radiation properties of different metal layers is a vertical stack of interconnects, joined by vias. We have chosen the dimensions of the interconnects in different layers following Intel's 32 nm technology node as listed in Table 3.1 [99]. The cross-section of the targeted structure is shown in Figure 3.3, and the resulting model is shown in Figure 3.4. We use Ansoft HFSS, a finite element method (FEM) based EM simulator to solve Maxwell's equations in the system. The excitation to the system is provided via a lumped port in HFSS between the bottom-most metal layer and a perfect electric conductor (PEC) plate functioning as a ground. This style of excitation is similar to the feed of a dipole antenna, and is justified due to the similarity of the system to an infinitesimal dipole, as described in the preceding section. The length of each interconnect layer is taken to be 3 µm. A sphere of radius 1 mm (represents close proximity of the attacker to the IC) enclosing the interconnect stack is used as the simulation region to limit the analysis within a finite volume. A radiation boundary is applied at the surface of the spherical region to eliminate reflection of incident radiation from the outer surface of the simulation region.

Electric Field Analysis: Contribution of Metal Layers

This interconnect stack system is excited at 1 GHz and the electric field amplitude is measured with distance from the structure. The far-field radiation pattern, as shown in

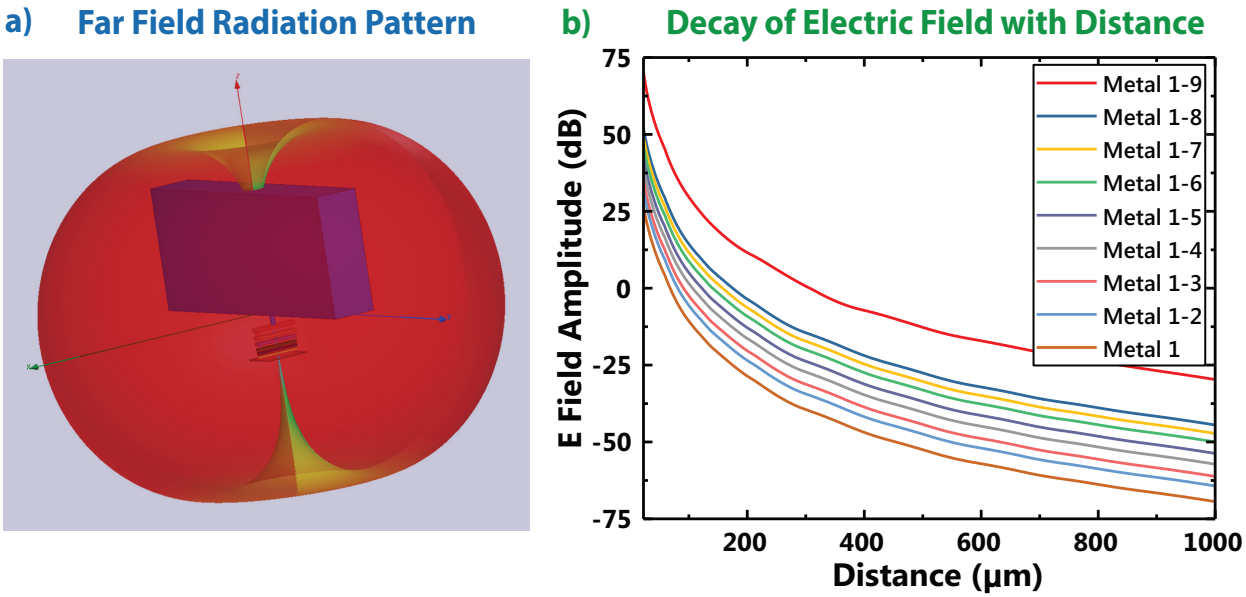


Figure 3.5. Simulation Results at 1 GHz excitation: Field Pattern. (a) Far-field radiation pattern, (b) E-field amplitude in dB (with reference at 1 V/m) vs distance for varying number of metal layers in the stack.

Figure 3.5(a), is analogous to that of a dipole antenna [98], as postulated earlier. We repeat the simulation multiple times, eliminating the topmost metal layer in each subsequent run, and examine the decay of radiated electric field with distance for each structure, as shown in Figure 3.5(b). This allows us to estimate the radiation contribution of each individual metal layer. For example, the difference between the E-field amplitudes obtained for M_{1-9} and M_{1-8} provides an estimation of the radiation emanated from metal layer 9. Note that, for the interconnect stack model under consideration, H-field is negligible in the near field, while E-field is dominant. This is because, electrically activated plates dominate the E-field in the near-field region, whereas current through loops creates more H-field in the near-field. Hence, for closed loop differential elements in a chip, H-field would be dominant in near-field which can be examined using similar analysis.

3.4 E-field Leakage detection from the metal layers: Simulation Results

To quantify the contribution of each layer at a particular distance from the probe (D), we utilize the simulated field amplitudes for the metal layer combination at $D = 900\mu m$

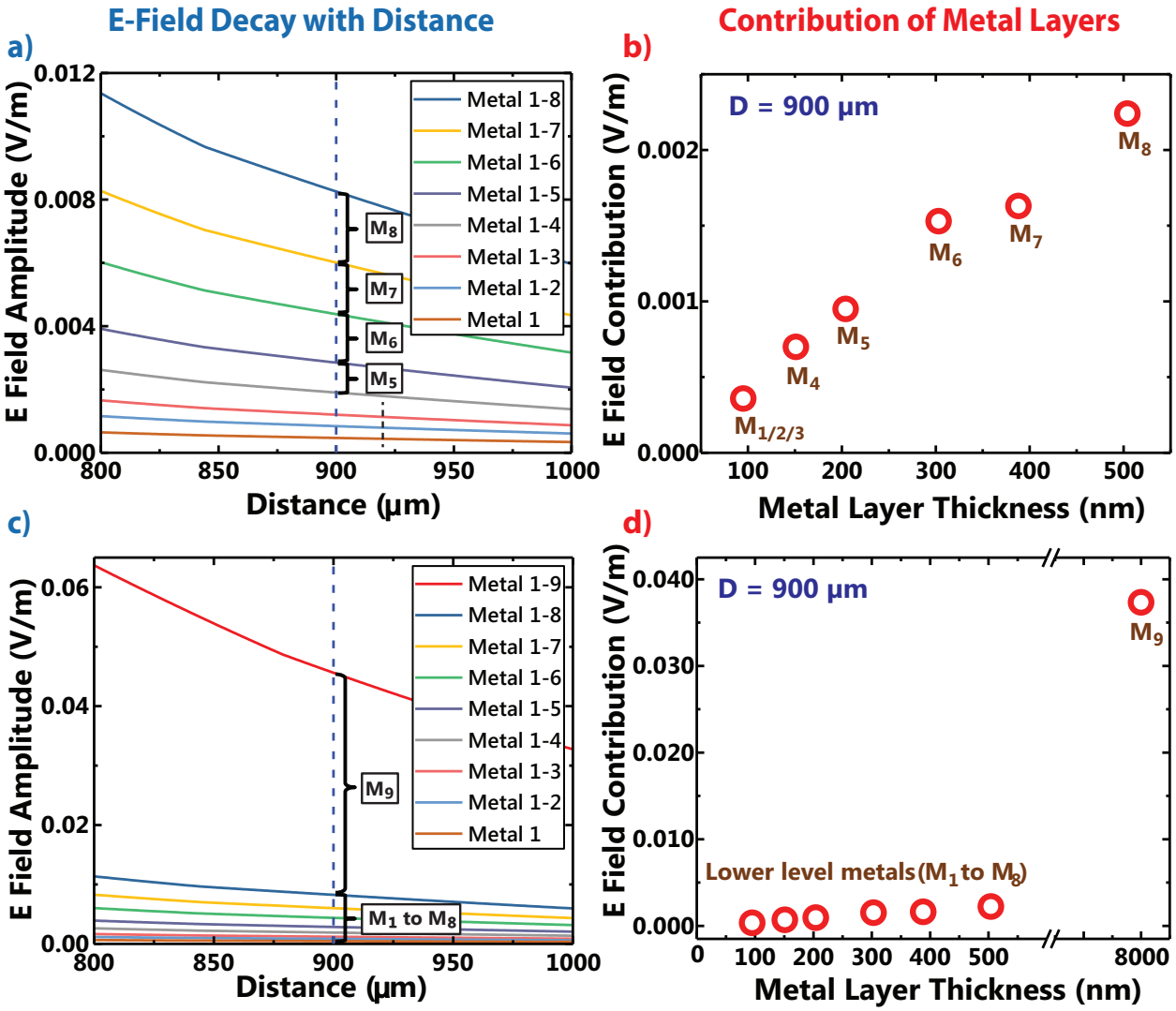


Figure 3.6. (a) E-field amplitude for the metal stack (layers 1 through 8) reduces as each layer is eliminated, (b) Contribution of Metal Layers 1 to 8, showing a linear relation with the dimension of the metal layers. (c, d) E-field contributions of the metals 1 through 9.

(Figure 3.6) and compute the difference between adjacent traces. The individual contribution of the layers to the E-field show a strong linear correlation with the dimensions of the metal layers. This is shown in Figure 3.6(a, b) where E-field contributions of M_1-M_8 is plotted against the thickness of those layers. The thickness of M_9 increases by a factor of 16 compared to M_8, and this translates into a significant E-field contribution from M_9 alone, as seen from Figure 3.6(c, d).

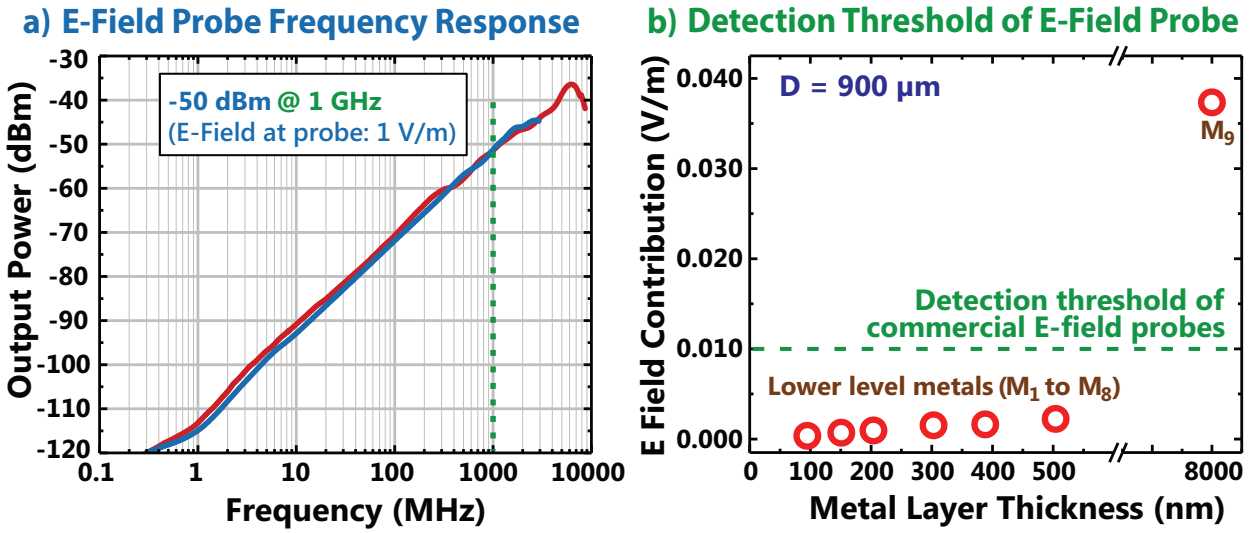


Figure 3.7. Sensitivity of the commercial EM Probes: (a) Frequency Response of a commercial E-Field probes (Probe 1 [100], Probe 2 [101]), (b) At $D = 900\mu m$, a commercial E-field probe can potentially detect radiation from Metal Layer 9 (Intel 32 nm process).

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

Accordingly, the detectable EM leakage from the metal layers can be formulated in terms of the noise floor ($NF_{oscilloscope}$) of the oscilloscope, the transfer function of the radiated electric field (E) to the current (I) flowing through the interconnects for different metal layers (M_X) and the response of the E-field probe (Figure 3.7), as shown in Eqn. 3.2. Note that, E_I represents the electric field generated due to the AES current.

$$\mathrm{i}_{AES}\left(E_I\right)_{M_X}\left(V_E\right)_{probe} \geq NF_{oscilloscope} \tag{3.2}$$

The total electric field measured by the external probe is the sum of contribution from the AES engine ($E_{I_{local}}$) and the unrelated logic ($E_{I_{global}}$) present in the circuit, as given in Eqn. 3.3. $E_{I_{global}}$ is the electric field from the global chip routing, whereas $E_{I_{local}}$ is from the local routing of the AES engine. Hence, typically, the AES engine is a small portion of the whole chip, that is, $E_{I_{global}} \gg E_{I_{local}}$.

$$E_I = E_{I_{local}} + E_{I_{global}} \tag{3.3}$$

The E-field E_I is measurable as long as the output voltage from the E-field probe (depending on the V_E transfer function of the probe) is above the noise floor of the oscilloscope (typically, $NF_{oscilloscope}$ is $\sim -90dBm$ at 1 GHz). Hence, as seen in Figure 3.7(a, b), the detectable E-field is $\sim 10mV/metre$, which means that E-field leakage from the metals up to the layer 8 in Intel 32 nm technology is not detectable.

It is to be noted that the analysis of the interconnect stack has been performed at 1 GHz where the EM probes have high sensitivity (Figure 3.7(a)), and hence encryption engines running at lower clock frequencies will have less detectable leakage as the probe sensitivity reduces at lower frequencies. Also, depending on the technology process, different metal layers may radiate above the detectable threshold. Based on these observations, we propose *STELLAR* around the crypto IP with local low-level metal routing, which attenuates the signature before it reaches the higher metal layers, and thus provides EM SCA immunity as discussed in the subsequent sections.

3.5 *STELLAR*: A Low Overhead Generic Countermeasure against EM SCA

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

In this regard, if we can somehow completely "shield" the top metal layer (M_9 for our example with Intel 32nm process) by suppressing the encryption signature even before it

reaches M_9, then there would be no detectable EM leakage from the encryption IC. Thus, solving the EM SCA problem is reduced to solving the power SCA problem in the lower-level metal layers, that is, suppressing the AES signature completely before it reaches the top-level metal layers. Keeping this in mind, we revisit the existing power SCA countermeasures.

Power SCA countermeasures include power balancing, hardware masking, noise injection, and supply isolation. Power balancing logic implementations involve sense-amplifier based logic (SABL) [102], dual-rail circuits [103], and wave dynamic differential logic (WDDL) [104].

Algorithmic masking is a logic-level countermeasure that involves replacing each logic operation with a sophisticated one to obfuscate the power consumption, leading to high power and area overheads ($> 4\times$) [96], [105].

Physical countermeasures include noise injection, switched capacitors, integrated voltage regulators (IVRs), and attenuated signature noise injection (ASNI). Noise injection alone incurs very high power overheads ($> 15\times$ to achieve MTD of $50K$) [87], [41] and is not an optimum solution. The switched capacitor current equalizer module proposed by Tokunaga et al. [106] is a novel technique against power SCA, however it resulted in a $2\times$ performance degradation in addition to the 33% power overhead. IVR-based implementations utilize traditional low-dropout regulators (LDOs) [107] and buck converters [108]. However, IVRs require large passives and thus consume $> 2\times$ power and area overheads, and use the bond-wire inductances, which can leak critical information in the form of EM emanations. Hence, this IVR-based countermeasure cannot be directly used for protecting against EM SCA.

Recently, Attenuated Signature Noise Injection (ASNI) has been proposed as a low-overhead generic countermeasure against power SCA [42]. It embeds the AES engine in a Signature Attenuating Hardware (SAH) which highly suppresses the variations in the AES signature with significantly low overhead. As the AES signature gets attenuated by $> 200\times$, a very small noise injection can decorrelate the power traces so that the traces obtained by probing at the observable power pin of the encryption ASIC are independent of the AES transitions ($MTD > 1M$). ASNI reduces the signal-to-noise ratio (SNR), both by strongly suppressing the signature, followed by tiny noise injection. However, ASNI is a power SCA countermeasure and does not constrain the placement or routing within the IC.

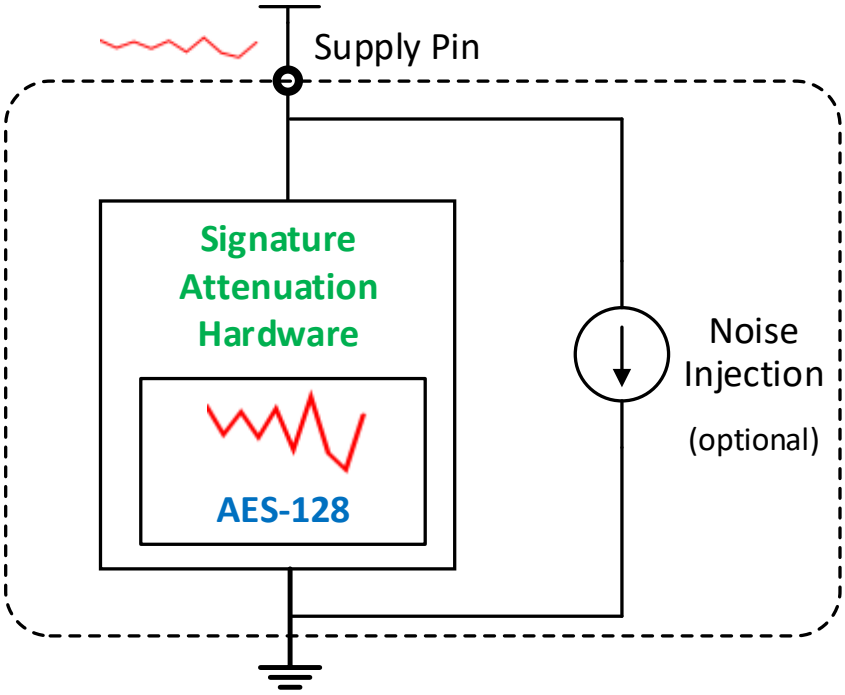


Figure 3.8. Overview of the Attenuated Signature Noise Injection (ASNI) AES [42]. Note that the additional noise injection is not necessary if the attenuated crypto signature is lower than the pre-existing noise in the sytem, which arises from the uncorrelated switching currents from other circuit blocks and the input referred noise of the measurement system.

3.5.1 Background: Attenuated Signature Noise Injection (ASNI)

Figure 3.8 shows an overview of the ASNI circuit. The underlying idea of ASNI is to embed the encryption engine (AES) in a signature attenuating hardware (SAH), such that the variations in the AES current is highly suppressed and is not reflected in the supply current traces, thereby requiring significantly lower noise current injection to decorrelate the measured supply traces [42].

ASNI uses SAH to attenuate (attenuation factor = AF) the AES signature so that the supply current (I_{CS}) becomes highly independent (high attenuation: $AF \rightarrow 0$) of the AES signal transitions. Here, it should be noted that the MTD is inversely proportional to the signal-to-noise ratio (SNR), as seen from Eqns. 3.12, 3.13 [109], [110], where k_1 is the

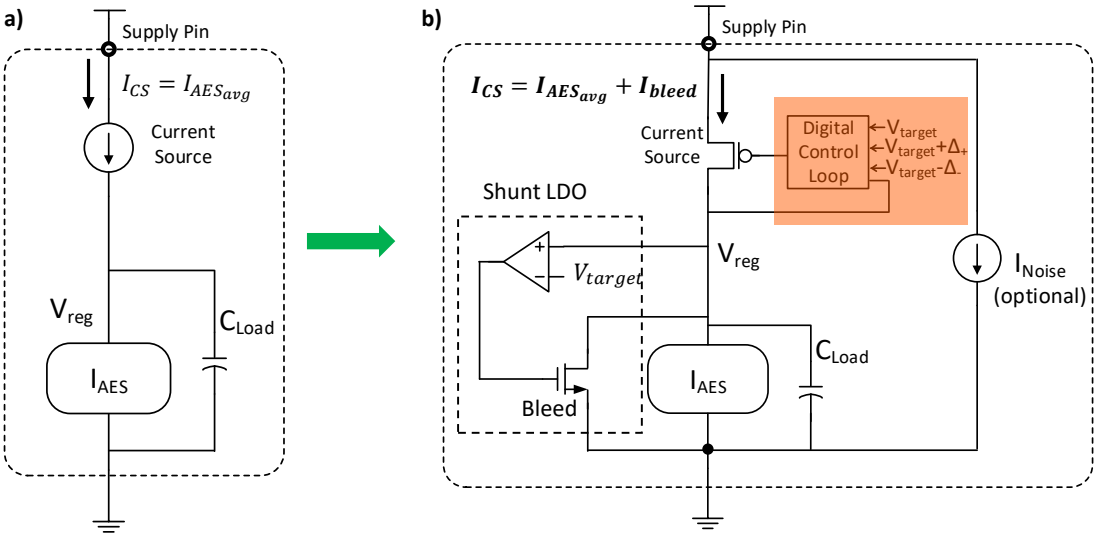


Figure 3.9. Background Work: Build-up to the SAH: (a) An ideal implementation, (b) ASNI-AES architecture with Signature Attenuation and Noise Injection to defend against power side-channel attacks [42].

success-rate dependent co-efficient, and $AT = \frac{1}{AF}$ represents the attenuation due to the SAH.

$$MTD = k_1 * \frac{1}{\rho_{TH}^2} \approx k_1 * (1 + \frac{1}{SNR}) \tag{3.4}$$

$$SNR = \frac{\sigma_T^2}{\sigma_{Noise}^2} = \frac{\sigma_T^2/AT^2}{\sigma_{N_{existing}}^2 + \sigma_{N_{add}}^2(optional)} \tag{3.5}$$

It is to be noted that the additional noise (N_{add}) is not necessary if the attenuated crypto signature is lower than the pre-existing noise ($N_{existing}$) present in the system arising due to the uncorrelated switching from other circuit blocks and the input referred noise of the measurement system.

The build-up to the SAH is shown in Figure 3.9. Figure 3.9(a) shows an ideal implementation involving an ideal constant current source on top of the AES engine, with an integrating load capacitor (C_{Load}) to account for the differences in the constant supply current and the variable AES current. This ideal topology only works if the constant current source supplies the average AES current $i_{AES_{avg}}$ over time. However, practically it is not fea-

sible since if $I_{CS} > \mathrm{i}_{AES_{avg}}$, the output voltage ($V_{reg}$) approaches V_{DD} (supply voltage) with time, due to the integration effects of the load capacitor, without any voltage regulation. Again, when $I_{CS} < \mathrm{i}_{AES_{avg}}$, the output voltage ($V_{reg}$) approaches $0V$ with time, without any regulation. Hence, the constraint that the supply current needs to be set to the average AES current is not practical and leads to a meta-stable state of operation without ensuring proper regulation of the output voltage, leading to a performance hit.

Hence, as shown in Figure 3.9(b), a shunt low-dropout (LDO) regulator loop with a bleed device (NMOS) is used to dissipate the overhead residual current (I_{bleed}) and thus acts as a correction mechanism to compensate for the integration effects of the load capacitor, as shown in Figure 3.9. This topology called the shunt LDO-based control loop senses V_{reg} and controls the bleed NMOS gate voltage to draw the difference of current between I_{CS} and I_{AES}. Thus, this circuit is able to simultaneously regulate V_{reg} while keeping I_{CS} independent of I_{AES}, thereby providing a significant time-variant attenuation by switching between small-signal and large-signal domains.

Another switched-mode control (SMC) digital loop tracks the large changes in the average AES currents and compensates for any process, temperature or voltage variations. However, once the supply current is set, the SMC digital loop is disengaged (grayed out in Figure 3.9(b)) in the steady-state operation of the SAH.

3.5.2 Proposed *STELLAR* Technique

We propose ***STELLAR*: Signature aTtenuation Embedded CRYPTO with Low-Level metAl Routing**, which utilizes a Signature Attenuating Hardware (SAH), such as the ASNI circuit, with local low-level metal routing around the crypto IP and suppresses the critical signature before reaching the topmost metal layers which radiate significantly.

Figure 3.10 shows the proposed *STELLAR* hardware with the crypto IP routed within the local low-level metal layers 1 through 7, which then connects to the global higher metal layer 9 (whose leakage is detectable by commercial probes) through the SAH in the form of ASNI. Hence, STELLAR locally embeds the AES-128 core with low-level routing, suppresses

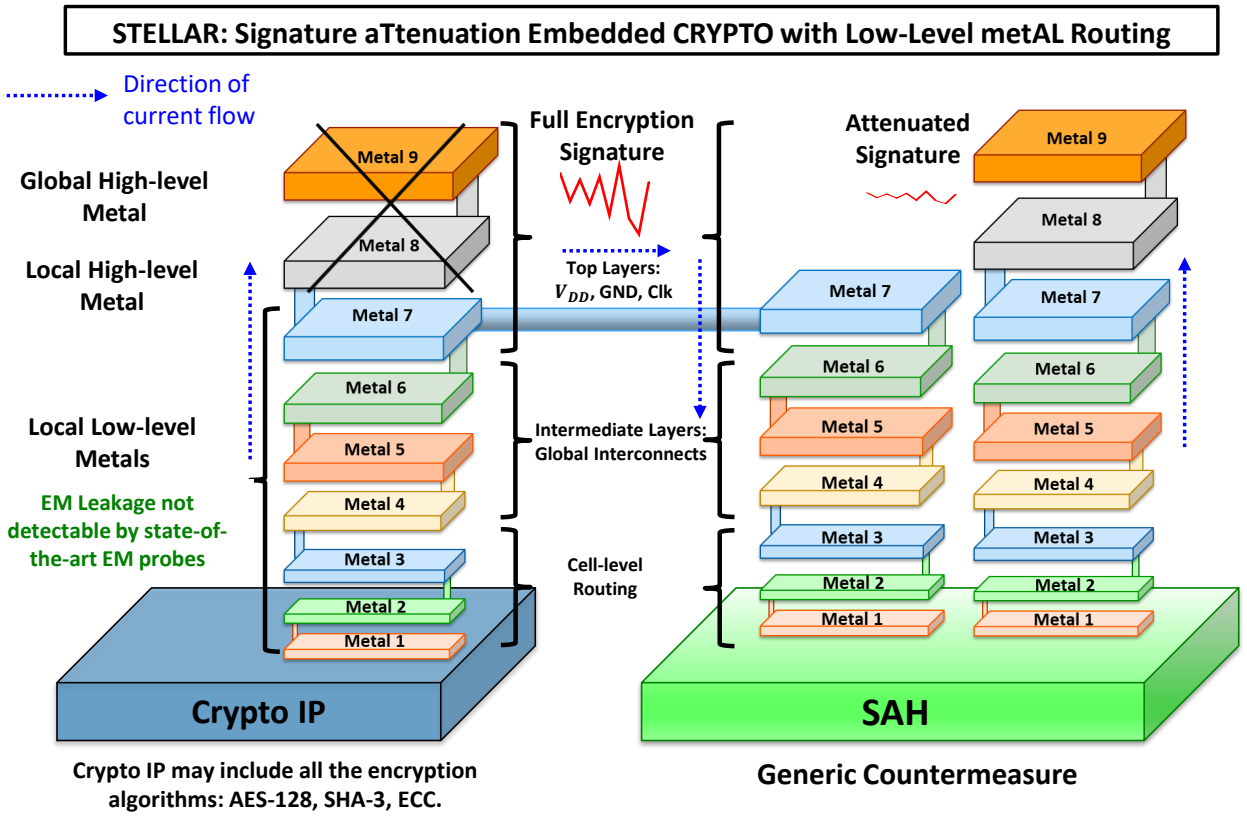


Figure 3.10. Proposed Stellar Technique with local SAH around the crypto block with low-level metal routing for EM Side-Channel Attack Protection.

the signature through ASNI and routes the attenuated signature through to the global higher metal layers, which is finally connected to the metal pads, as illustrated in Figure 3.11(a).

Figure 3.11(a) shows the routing strategy in a smart card, where the crypto signals are routed within the lower metal layers. However, these signals have to come through the external pins to connect to the supply, and those power routing is done through the higher metal layers, which is the root-cause of the EM leakage as we studied in Section 3, 4. Hence, only local signal routing does not prevent EM leakage, and hence a signature attenuation hardware (SAH) is necessary.

Figure 3.11(b) shows that the ASNI circuit with high-level long metal routing with the crypto block although attenuates the current signature from reaching the power pin using the SAH, but does not prevent EM side-channel leakage.

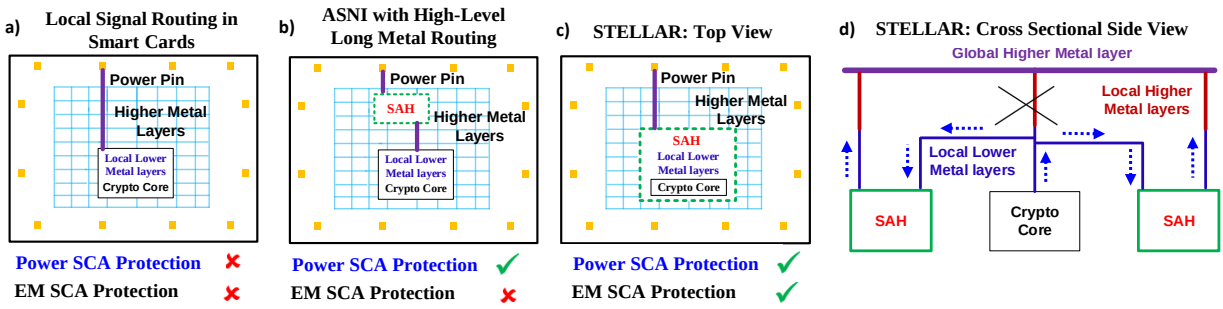


Figure 3.11. (a) Low-level metal layer Signal Routing traditionally used in smart-cards does not reduce EM leakage as the signals have to come through the higher level metals to connect to the external pin, (b) ASNI with high-level long metal routing prevents power SCA, but not EM SCA, (c) STELLAR technique utilizing the SAH block around the crypto IP locally routed with low-level metal layers and the attenuated signature flows through the leaky high-level metals, (d) Cross-sectional side-view of the STELLAR shows that the higher metal layers are isolated from the crypto core, thus carrying a highly suppressed encryption signature after being passed through the SAH (ASNI) circuit.

Hence, we propose *STELLAR* (Figure 3.11(c)), which utilizes the SAH locally around the crypto block with low-level metal routing and attenuates the current signature within the lower metal layers, and thus prevents any detectable EM leakage from the higher metal layers (carrying the attenuated power signatures) which connects to the external pins.

The cross-sectional block-level layout of the STELLAR (Figure 3.11(d)) shows the current flow through the metal layers connecting the crypto core and the SAH with the metal layers. The crypto core locally embedded within the SAH is routed using the local lower metal layers, which in turn connects directly to the global higher metal layers.

STELLAR uses the SAH which provides high attenuation (1/AF) and the attenuation factor (AF) depends on the choices of the load capacitor (C_{Load}), amount of overhead bleed current (i_{bleed}), the gain of the op-amp (A_v), transconductance of the bleed NMOS (g_m), placement of the dominant pole of the op-amp (p), and also the output resistance (r_{ds}, $g_{ds} = 1/r_{ds}$) of the current source (PMOS) (refer Figure 3.9). Since an ideal current source is not feasible, a finite r_{ds} would reflect relative change in the output voltage (V_{reg}) into the supply current, however it will be highly attenuated ($> 200\times$), as seen from the time-domain waveforms of the STELLAR-AES (Figure 3.12). Hence, a tiny amount of random

noise current is injected (as shown in Figure 3.9(b)) to decorrelate the supply current traces with the estimated HD matrix, thereby providing significant immunity against CPA/CEMA attacks. The amount of noise injection required, as well as the total current overhead in the case of STELLAR-AES is quantitatively analyzed in Section VI.A.

3.6 *STELLAR*: Local ASNI around Crypto-IP with lower metal routing

In the previous section, we have investigated the power SCA countermeasures and proposed the STELLAR technique utilizing the ASNI circuit to provide significant attenuation to the AES signature with extremely low overheads. In Section 4, we have also analyzed that the EM emanations from metal 9 is detectable using commercial EM probes for the Intel 32 nm CMOS process. However, the threshold may vary depending on the particular CMOS process, as discussed earlier. Hence, if we "shield" the high-level metal layers (M_9 in this case) by encapsulating the locally-routed AES engine with the ASNI hardware (Figure 3.10, 3.11), then the AES signature cannot be detected by an external EM attacker. Hence, we now evaluate the STELLAR hardware placed on top of the AES-128 core designed in TSMC 65 nm CMOS process [1].

In STELLAR, the placement of the AES core encapsulated by the ASNI circuit is very critical and has security, power and performance trade-offs. To achieve the highest level of security against EM SCA (maximum MTD), the ASNI along with the AES needs to be routed with the lowest metal layers. Although it provides maximum signature suppression (leading to the minimum noise injection overhead), lower metal layers suffer from high resistance and may result in a high voltage drop across the output voltage (V_{reg}), which can degrade performance (leading to lower throughput) of the AES encryption engine. The AES-128 core design consumes a physical chip area of $\sim 0.35mm^2$ [42]. Assuming that the maximum

[1]↑Note that, due to NDA reasons, we do not provide the metal stack information for TSMC 65 nm technology, in which the STELLAR design and simulations are carried out. The EM analysis is performed on the Intel 32nm process as the interconnect stack dimensions are publicly available [97].

length of routing is $L_{max} = 350\mu m * \sqrt{2} = 493\mu m$ and we can tolerate an output voltage drop of $10mV$, the maximum tolerable routing resistance (R_{max}) is given by Eqn. 3.6.

$$R_{max} = \frac{\Delta V_{max}}{\mathrm{i}_{AES_{avg}}} = \frac{10mV}{1mA} = 10\Omega. \tag{3.6}$$

$$R_{L_{max}} = \frac{R_{max}}{L_{max}} = \frac{10\Omega}{493\mu m} \approx 0.02\Omega/\mu m \tag{3.7}$$

Hence, we can route the STELLAR-AES core only with metal layers for which $R < R_{L_{max}} = 0.02\Omega/\mu m$ (Eqn. 3.7). Now, considering the Intel 32 nm CMOS process, only metals above layer 7 provides the desired low routing resistances and hence has no performance degradation in the operation of the cryptographic core. Thus, the AES can be routed up to metal layer 7 (as shown in Figure 3.10) and shielded with the ASNI hardware so that signals leaking to higher metal layers (M_8, M_9) are highly attenuated. However, the placement of the ASNI-AES core needs to be analyzed in design-time depending on the particular process (CMOS technology). STELLAR using the local ASNI provides an attenuation ($\frac{1}{AF}$) to the AES signature such that the measured electric field (Eqns. 3.2, 3.3) gets modified accordingly as shown in Eqns. 3.8, 3.9, 3.10.

$$E_{I_{STELLAR}} = \frac{E_{I_{local}}}{AT_{local}} + \frac{E_{I_{global}}}{AT_{global}} \tag{3.8}$$

$$AT_{local} = \frac{M_9}{M_{X_{Crypto}}} : \textit{E-field reduction due to absence of higher local metal layers} \tag{3.9}$$

$$AT_{global} = \frac{1}{AF_{SAH}} : \textit{AES Signature Suppression using SAH} \tag{3.10}$$

Hence, as seen from Eqns. 3.9, 3.10, the overall SNR reduction has two key components: (1) Electric field suppression (AT_{local}) achieved due to the absence of routing through the

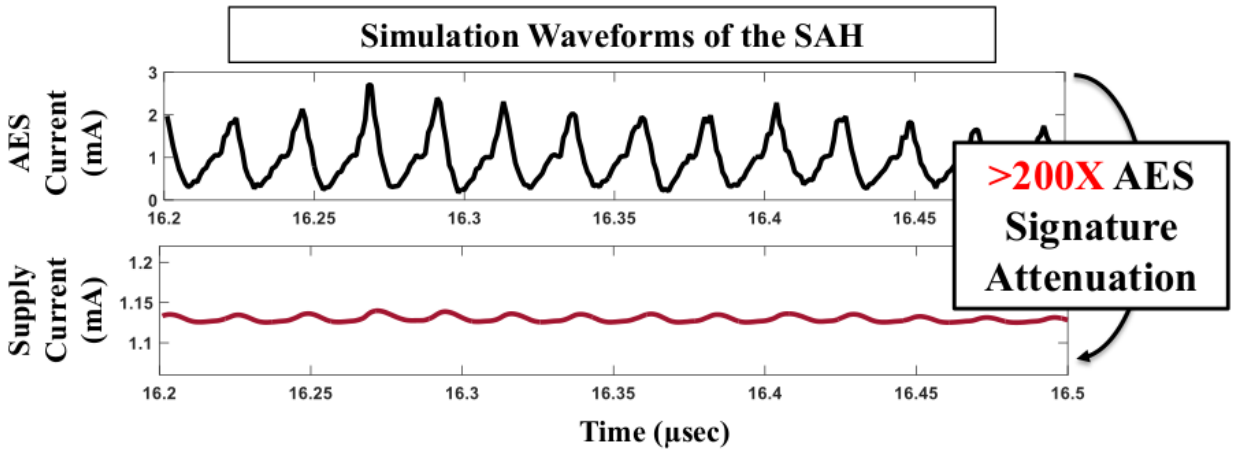


Figure 3.12. Snapshot of the time-domain waveforms of the signature Attenuation hardware utilized by the STELLAR-AES.

local high-level metal layers (M_8 in our case, refer Figure 3.10). In this case, if the AES-128 core embedded within the SAH (ASNI) block is routed with local low-level metal M_1 to M_7 (meeting the constraint presented in Eqn. 3.6, 3.7), the ASNI hardware can then directly connect to the global high-level metal M_9, and thus $AT_{local} = \frac{M_9}{M_7} \approx 20$ (from Table 3.1). (2) AES Signature suppression (AT_{global}) using SAH ensures that although the EM signal leakage from the global metal layers remain the same, the correlated signature present in the emanated E-field is significantly attenuated.

Now, the ratio of the electric fields contributed by the local and global routing from the AES block can be attributed to the relative area of the AES to the area of the rest of the circuit (refer Figure 3.11 (a) - the higher metals form a mesh structure throughout), as given in Eqn. 3.11,

$$\begin{aligned} \frac{E_{I_{local}}}{E_{I_{global}}} &= \frac{\text{Area of AES}}{\text{Total Chip Area - Area of AES - Area of pads}} \\ &\approx \frac{200\mu \times 200\mu}{1m \times 1m - 200\mu \times 200\mu} = \frac{1}{24}. \end{aligned} \tag{3.11}$$

Now, from Eqn. 3.3 and Figure 3.6(a), we see that for an excitation of 1V with 50 Ω termination (i = $20mA$), $E_{I_{local}} + E_{I_{global}} = 35mV/m$ at a probe distance of $900\mu m$. This

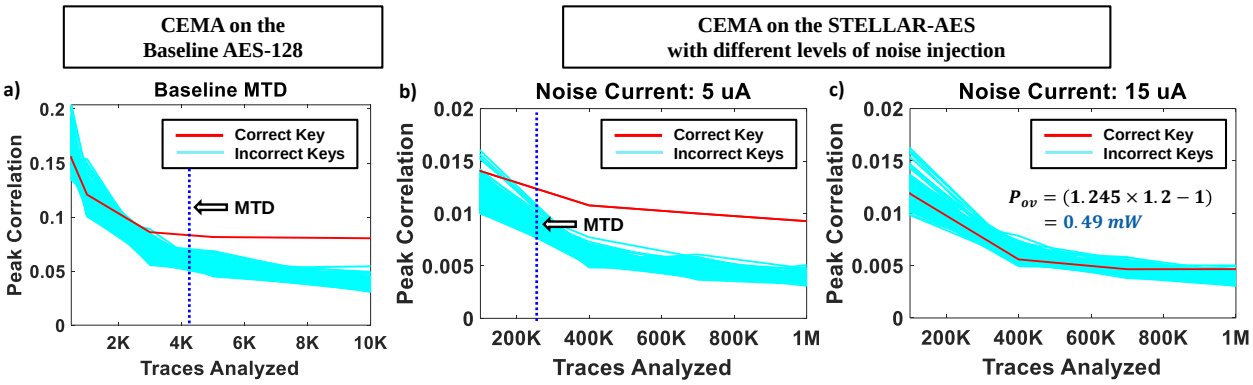


Figure 3.13. MTD Analysis: (a) Minimum Traces to Disclosure (MTD) for a CEMA attack on the baseline AES-128 implementation, (b, c) Locally-routed STELLAR-AES: Noise Injection on the modified AES in Attenuated Signature domain, to achieve MTD of 1 Million traces.

translates to an electric field of $E_I \approx 6mV/m$ for our case with an AES peak current $\mathrm{i}_{AES_{max}} = 3.2mA$. Using Eqn. 3.11, we obtain $E_{I_{local}} = \frac{1}{24} * 6 = 0.25mV/m$ and $E_{I_{global}} = \frac{23}{24} * 6 = 5.75mV/m$.

As the STELLAR hardware is embedded on top of the AES-128 encryption engine, using Eqns. 3.8, 3.9, 3.10 the measured electric field becomes $E_{I_{STELLAR}} = \frac{0.25}{20} + \frac{5.75}{200} \approx 0.04mV/m$, which means that the effective suppression of the AES signature is $\sim 150\times$.

3.6.1 Results & Overhead Comparison

We perform CEMA attack on the AES-128 core (1^{st} round S-Box operation) with a clock frequency of 40 MHz and an average current ($I_{AES_{avg}}$) of $\sim 1mA$ (peak current = 3.2 mA). The AES-128 engine performs one block encryption in 10 cycles. The CEMA attack reveals the secret key of the unprotected AES within $< 6K$ traces (Figure 3.13(a)), whereas the same attack on the STELLAR-AES does not reveal the secret key even with $1M$ traces (Figure 3.13(c)).

Figure 3.13(b, c) shows the evolution of the MTD with different levels of noise injection after the signature attenuation of the locally routed AES engine (STELLAR-AES). Figure 3.13(c) shows that only $15\mu A$ of noise current injection is required to achieve Minimum Traces to Disclosure (MTD) $> 1M$.

Now, the minimum traces to disclosure (MTD) is inversely proportional to the signal-to-noise ratio (SNR) of the attack, as seen from Eqns. 3.12, 3.13 [109], [110], where k_1 is the success-rate dependent co-efficient.

$$MTD = k_1 * \frac{1}{\rho_{TH}^2} \approx k_1 * (1 + \frac{1}{SNR}) \tag{3.12}$$

$$SNR = \frac{\sigma_T^2}{\sigma_{Noise}^2} = \frac{\sigma_T^2/AT^2}{\sigma_{Noise}^2} \tag{3.13}$$

Using Eqns. 3.12, 3.13, the relation between MTD, ASNI signature attenuation factor (AF_{ASNI}) and the overall noise (I_{Noise}, includes the pre-existing system noise) is given by Eqn. 3.14.

$$MTD \propto \frac{1}{SNR} \propto (AT * I_{Noise})^2 \propto \left(\frac{I_{Noise}}{AF_{ASNI}}\right)^2 \tag{3.14}$$

Hence, for a higher MTD, more noise may be injected or the attenuation (AT) may be enhanced, which could be achieved by the lower-level routing (increasing AT_{local}), or by increasing the ASNI circuit attenuation ($AT_{global} = \frac{1}{AF_{ASNI}}$). With the same level of attenuation, the amount of noise current required to achieve MTD of 100M would be $I_{Noise} \sim 15\mu A * \sqrt{\frac{100M}{1M}} = 150\mu A$.

The current consumed by the amplifier in the shunt LDO loop consumes a current of $\sim 100\mu A$ and hence the total overhead current is given as $I_{ov} = I_{bleed} + I_{noise} + I_{opamp} = 130\mu A + 15\mu A + 100\mu A \approx 0.24mA$. Thus, to achieve a $MTD > 1M$ the total overhead power for the STELLAR-AES architecture is $(1.13mA + 0.015mA + 0.1mA) * 1.2V - 1mA * 1V = 0.49mW$. Power efficiency for STELLAR-AES is given as, $\eta = \frac{(1mA*1V)}{(1.245mA*1.2V)} * 100 \approx 67\%$ (includes noise overhead). Hence, STELLAR-AES consumes similar overhead as [18], but does not incur the performance penalty. Implementation of the SAH consumes an area of $\sim 0.08mm^2$, while a standalone AES incurs $0.35mm^2$, which implies an area overhead of $\sim 22.85\%$, for $MTD > 1M$.

3.7 Conclusion

Electromagnetic emission from cryptographic ICs is a prominent side-channel attack vector to extract the secret key without physical access to the device. The growth of internet-connected small form-factor devices and the availability of cheap commercial EM probes calls for an efficient countermeasure against EM SCA. This chapter, for the first time, performs a white-box modeling of the interconnect metal-via stack within an integrated circuit which leaks critical signal transitions in the form of EM radiation. System-level modeling of the interconnect structure for Intel 32 nm CMOS process reveals that metals above layer 8 leak the most and can be detectable using commercially available cheap EM probes. This work proposes the STELLAR technique to locally route the AES-128 encryption engine in the lower-level metal layers and also encapsulated within a low-overhead signature suppression hardware (ASNI). The ASNI circuit is then routed to the leaky higher-level metals, which now contains only the suppressed AES signatures. Hence, using STELLAR with local low-level metal routing along with the SAH as an efficient"shield" protects the AES-128 encryption signatures from radiating, thereby achieving $MTD > 1M$ with only a tiny noise injection of $15\mu A$. STELLAR with low-level metal routing with the SAH (ASNI) local encapsulation around the crypto block not only provides a low-overhead solution ($1.5\times$ power, $1.23\times$ area overhead) against EM SCA, but it is also a generic countermeasure and can be extended to other cryptographic engines.

In the next chapter, based on our understandings of the white-box analysis of the EM leakage, we will look into a reduced EM leakage cell design for enhanced SCA security.

4. EM SCA WHITE-BOX ANALYSIS BASED REDUCED LEAKAGE CELL DESIGN & PRE-SILICON EVALUATION

A version of this chapter is currently under review:
1. Debayan Das, Mayukh Nath, Baibhab Chatterjee, Raghavan Kumar, Xiaosen Liu, Harish Krishnamurthy, Manoj Sastry, Sanu Mathew, Santosh Ghosh, Shreyas Sen, EM SCA White-box Analysis Based Reduced Leakage Cell Design and Pre-Silicon Evaluation.

This chapter presents a white box modeling of the electromagnetic (EM) leakage from an integrated circuit (IC) to develop EM side-channel analysis (SCA) aware design techniques. A new digital library cell layout design technique is proposed to minimize the EM leakage and is evaluated using a high frequency structure simulator (HFSS)-based framework. Backed by our physics-based understanding of EM radiation, the proposed double-row power grid based digital cell layout design shows $> 5\times$ reduction in the EM SCA leakage compared to the traditional digital logic gate layout design. Further, exploiting the magneto-quasistatic (MQS) regime of operation of the EM leakage from the CMOS circuits, the HFSS-based framework is utilized to develop a pre-silicon (Si) EM SCA evaluation technique to assess the vulnerability of cryptographic implementations against such attacks during the design phase itself.

4.1 Background

The increasing demand of internet-connected and miniaturized devices calls for stringent security requirements which has led to the development of robust and mathematically-secure cryptographic algorithms like AES, SHA, RSA. These classical cryptographic algorithms are responsible for providing confidentiality, integrity, and authenticity in critical platform features like secure boot, trusted platform module (TPM), secure debug, and so on, and hence they are designed to be highly resilient against probabilistic polynomial time (PPT) attackers. However, over the last two decades, many of these algorithms have been broken by taking advantage of its underlying physical implementation to recover secret parameters

like the encryption key utilizing what is known as side-channel analysis (SCA) [111]. In this work, we focus on electromagnetic (EM) SCA attacks, which is a non-invasive attack on embedded electronic devices to recover the secret key [112], [90].

4.1.1 Motivation

Recently, it was shown that the AES-256 encryption key could be broken in just five minutes from a distance of 1 meter [113]. Most commercial devices today are transitioning from AES-128 to AES-256 for encryption to provide enhanced data security. Although AES-256 provides exponential improvement in the computational security compared to AES-128, the side-channel security only increases linearly [43], [44]. Several practical side-channel attacks using simple/differential/correlational EM analysis (SEMA/DEMA/CEMA) [112], [90], on crypto devices have been demonstrated over the recent years. Moreover, the continuous advancement of the low-cost high-resolution EM probes is increasing the threat surface of the embedded devices significantly. Hence, it becomes extremely imperative to protect against these EM SCA attacks.

Most prior works on EM SCA countermeasures treat the crypto engine as a black box without analyzing the root-cause of the EM leakage. Hence, the solutions typically involve high overheads in terms of performance, power, and area. This work treats the cryptographic hardware as a white-box and proposes EM leakage reduction techniques during the design phase itself. In our recent works, it has been shown that the root-cause of the EM leakage from the crypto hardware implementation depends significantly on the higher-level metal layers as they behave as more efficient antennas [37], [40]. In this work, we deep-dive into the individual logic gate designs and investigate their layouts to provide insightful and intuitive design guidelines to minimize the EM radiation.

Moreover, it should be noted that, till now, most of the EM analysis and evaluation of a countermeasure is performed only after the chip has been fabricated, that is, in the post-silicon (Si) phase, since the EM leakage could not be measured without the physical chip. Only a few recent works exist on developing a pre-Si EM SCA evaluation framework [114], [93], [116]. The framework used in [93] is based on extracting the circuit currents from

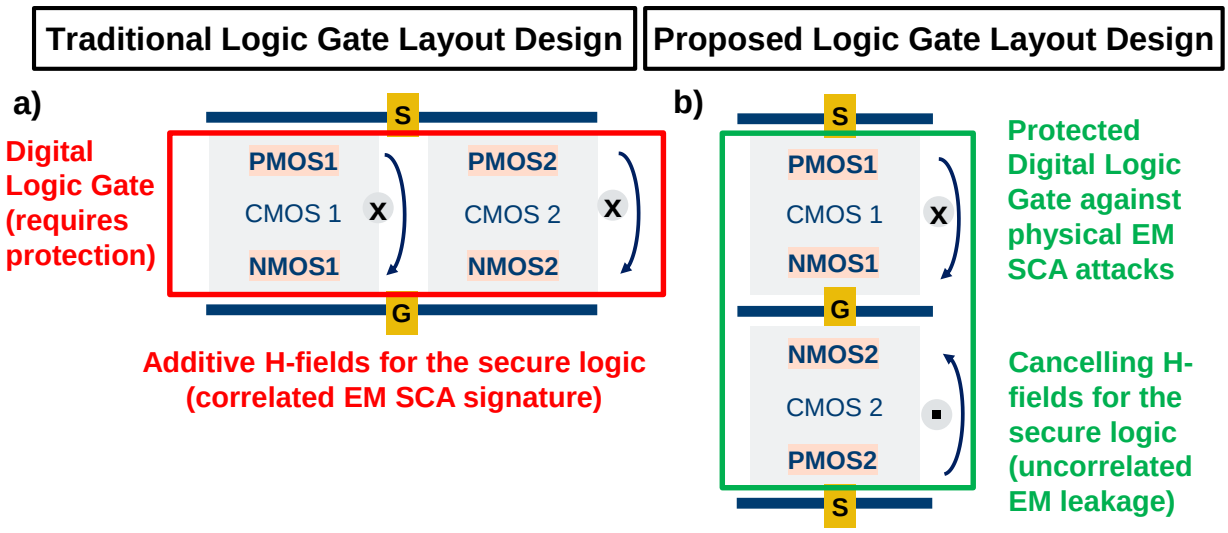


Figure 4.1. Key concept: (a) The conventional digital library logic cells are routed in the same row of the power grid (between supply (S) and ground (G) rails), and hence the current flow for the switching events are in the same direction, resulting in additive magnetic (H) fields, whereas, (b) the proposed digital library cell with the layout design split across two power grid rows (S, G, S) results in opposing currents in the alternating cell rows leading to cancellation in the H-field (which tends to be the dominant contributor to the EM leakage due to the formation of current loops in ICs [114], [115]), thereby minimizing the EM leakage significantly at the gate-level itself. This chapter builds a framework to analyze this key idea and extends this framework towards pre-silicon (Si) EM SCA evaluation.

Virtuoso and then using a custom-built framework for EM analysis through a theoretical modeling, which has not been validated through measurements. [114], [116] have used Redhawk which is a static IR-drop simulator followed by a custom-built framework for H-field approximation. These custom-built frameworks are not easily reproducible and hence we want to utilize the existing commercial EM analysis tools like the Ansys HFSS. However, HFSS in itself cannot simulate an entire crypto circuit because of the high complexity of the layout and the small geometries involved. Our goal is to exploit the MQS nature of the EM leakage from a crypto IC along with the white-box understanding of the EM leakage to optimally utilize commercial frameworks like HFSS (along with Virtuoso for the current extraction) which provides an accurate prediction of the EM SCA leakage from a crypto IC. Hence, in this work, we utilize the HFSS-based framework developed for our white-box

modeling to evaluate the resilience of the crypto implementations against EM SCA attacks prior to the fabrication, that is, in the pre-Si phase.

Overall, this work aims to provide EM SCA aware design strategies to protect against these EM attacks, develops a framework for the ground-up root-cause analysis, and simultaneously proposes to leverage this framework towards pre-Si EM SCA evaluation.

4.1.2 Contribution

The key contributions of this work are:

- Utilizing physics-level understanding of the near-field radiation from magnetic dipoles, the effect of the digital cell layout and the power grid is analyzed to provide insightful guidelines to the designer during the design phase itself prior to fabrication. Contrary to the conventional single-row layout of the standard digital library cells, we propose a double-row split-layout architecture across two rows of the power grid, showing a $> 5\times$ improvement in the radiated H-field (Section III, IV).

- An EM leakage evaluation framework for actual circuit layouts is developed using high frequency structure simulator (HFSS) by emulating the transistor switching events intelligently (using parameterized resistors) (Section III).

- Exploiting the MQS regime of the EM leakage from crypto circuits (given its frequency of operation and the geometry of the metal layers), the proposed framework can be leveraged towards evaluating the EM SCA attack resilience of crypto implementations in the pre-Si phase, thereby reducing the time-to-market significantly (Section V).

- The key concepts - EM SCA resilient design techniques through ground-up understanding and the pre-Si EM SCA evaluation are proven across two different processes (TSMC 65nm, Intel 10nm) and across two different set-ups (Purdue University, Intel Labs) (Section III-V).

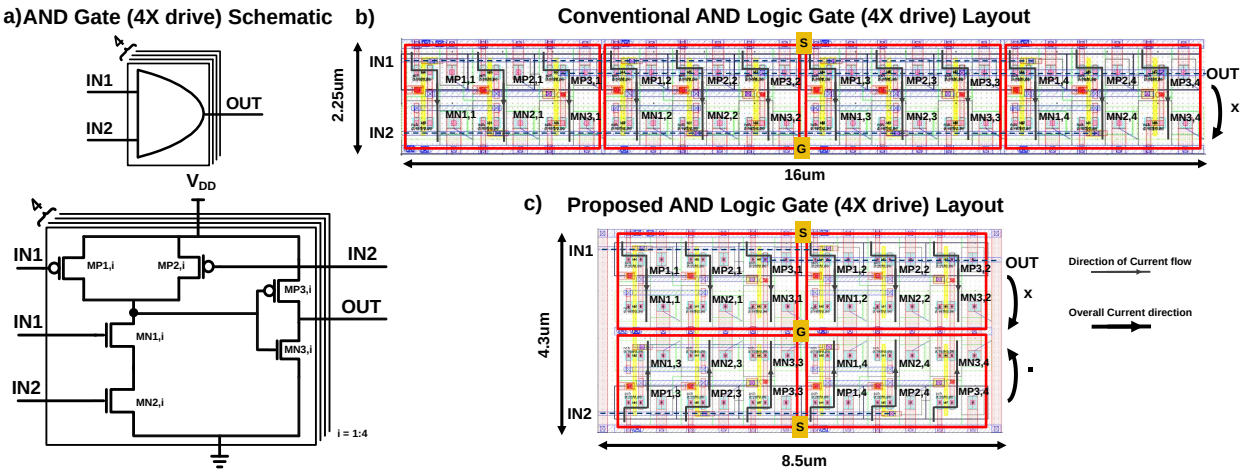


Figure 4.2. Different layout patterns of the same AND logic gate circuit under analysis: (a) Schematic of the AND logic gate with 4X drive strength, (b) single-row power grid (SG), which is the conventional cell layout, and (b) proposed double-row power grid (SGS). Both the layouts for the AND gate circuit have the same areas, and the key difference in the proposed double-row power grid (SGS) is that the transistors placed in alternate rows are flipped in contrast to the conventional digital cell structure. However, no overheads are incurred by adopting the SGS power grid in place of the SG for the library cells, and it remains agnostic of the circuit under analysis (generic to any crypto core).

4.2 Related Work

Over the last two decades, there have been significant advances in EM SCA, both in attacks as well as countermeasures. Many real-world attacks have been demonstrated on embedded devices to recover the secret key from its bootloader [13], [82]. Recently, SCA attacks have been demonstrated on bitcoin wallets to obtain the secret key of the device. In 2018, screaming side-channel was demonstrated, showing how the radio transmitter could radiate sensitive information regarding the digital logic on the same IC, leading to the recovery of the encryption key from a distance of up to 10 meters [33]. Fully-automated EM SCA attack framework (SCNIFFER) using gradient-search algorithm to detect high-leakage location on the target device have been proposed to accelerate these attacks [117]. In 2021, EM SCA attacks have been successfully performed on the iPhone devices to extract the hardware AES-256 secret key [27], as well as on the Google Titan security key [26]. Moreover, the

recent advancements in machine-learning (ML) based profiled SCA attacks have been shown to break various crypto implementations in much fewer traces compared to the conventional CEMA/DEMA-based non-profiled SCA attacks [34], [69], [35].

Consequently, various solutions to prevent EM and power SCA have been proposed, which can be broadly classified into three categories - architectural, logical, and circuit-level (physical). Architectural countermeasures include shuffling [118], random insertion of dummy operations, software masking, and data path obfuscation [119]. Logical countermeasures include sense amplifier based logic (SABL), wave dynamic differential logic (WDDL), and gate-level masking [96]. Circuit-level countermeasures include digital low-dropout (LDO) regulators [120], [121], switched capacitors [106], and signature attenuation [41], [42]. Most of these solutions are algorithm-specific and incur high area/power overheads. We need a low overhead generic countermeasure to prevent EM SCA attacks. Hence, a white-box analysis is critical to understand the source of the EM leakage from an integrated circuit (IC).

Recently, in 2019, a root-cause analysis of the EM leakage from crypto ICs was performed which revealed that the higher level metals are the main source of this radiation [37], [43]. Henceforth, signature attenuation with lower-metal routing was demonstrated to prevent EM SCA attacks for any crypto algorithm [37], [43]. This work extends the white-box modeling for real IC layouts and proposes layout modifications for the basic digital gates which would fundamentally provide more security benefits without incurring any additional overheads and agnostic of any crypto algorithm.

Such white-box analysis calls for an in-depth understanding of the EM generation on-chip, which when incorporated as a part of the design process could aid in the identification of the vulnerabilities in the pre-Si phase itself. Notably, most of these previous works evaluate the EM SCA in post-Si after the chip is fabricated. Previous works on modeling this EM leakage from an IC have used EM analysis tools like Redhawk for the static IR-drop simulation followed by an analytical modeling using Biot Savart's law to obtain the magnetic field heatmap for an IC [114], [116]. [114] showed a validation of the modeling by incorporating noise in the framework. Another recent work [93] uses transient analysis to obtain the transient currents from Virtuoso, but it requires extracting the current information from thousands of branches which is extremely tedious to perform manually. Once the currents

are obtained, the geometry information is extracted from the parasitics and then an analytical modeling is performed using the Maxwell's equations. Both these works [93], [116] have used theoretical equations to model the EM leakage without the use of commercially-validated tools to reduce complexity. Moreover, a static IR-drop based approach does not emulate the transient switching behavior of the transistors, and hence the electric (E)-field & magnetic (H)-field signatures in an IC. Further, none of the prior works have validated these custom-built models with commercial 3D Finite element method (FEM) simulators like Ansys HFSS. However, the main challenge is that HFSS cannot directly simulate an entire integrated circuit layout due to the high complexity of metal structures and the requirement of extensive graphics support. Even if it is able to simulate a full small circuit, it would take much longer than the prior works based on custom-built models. Recently, DARPA Side Channel Attack Testbench Estimator (SCATE) program has called for such pre-Si SCA evaluation framework development that can be performed in 24 hours. Keeping this in mind and utilizing the key insights from our physics-based white-box understanding and the MQS nature of the EM leakage, we develop a pre-Si EM SCA framework using the commercial tools (Virtuoso + HFSS) to make simulations feasible and faster.

Hence, in this work, along with the white-box analysis to develop EM SCA aware design techniques for the digital logic gates, we utilize the proposed HFSS-based framework towards building a pre-Si EM SCA evaluation technique that would be useful in analyzing the resiliency of crypto algorithms, as well as countermeasures, prior to the chip fabrication.

4.3 White-Box Modeling & Framework for the EM Leakage Analysis

In this section, we will discuss the white-box modeling of the EM leakage from an IC and explore design techniques to counter EM SCA.

This chapter focuses on H-field analysis instead of E-field since the formation of current loops on an IC (forming H-field) is much more prominent than the effect of metal layer surfaces (creating E-field) [115]. This is corroborated by many of the prior works [114], [93], [116], which have thus focused on H-field analysis as well. Also, the operating frequencies of the CMOS circuits have been limited to $< 10GHz$ primarily due to the power density

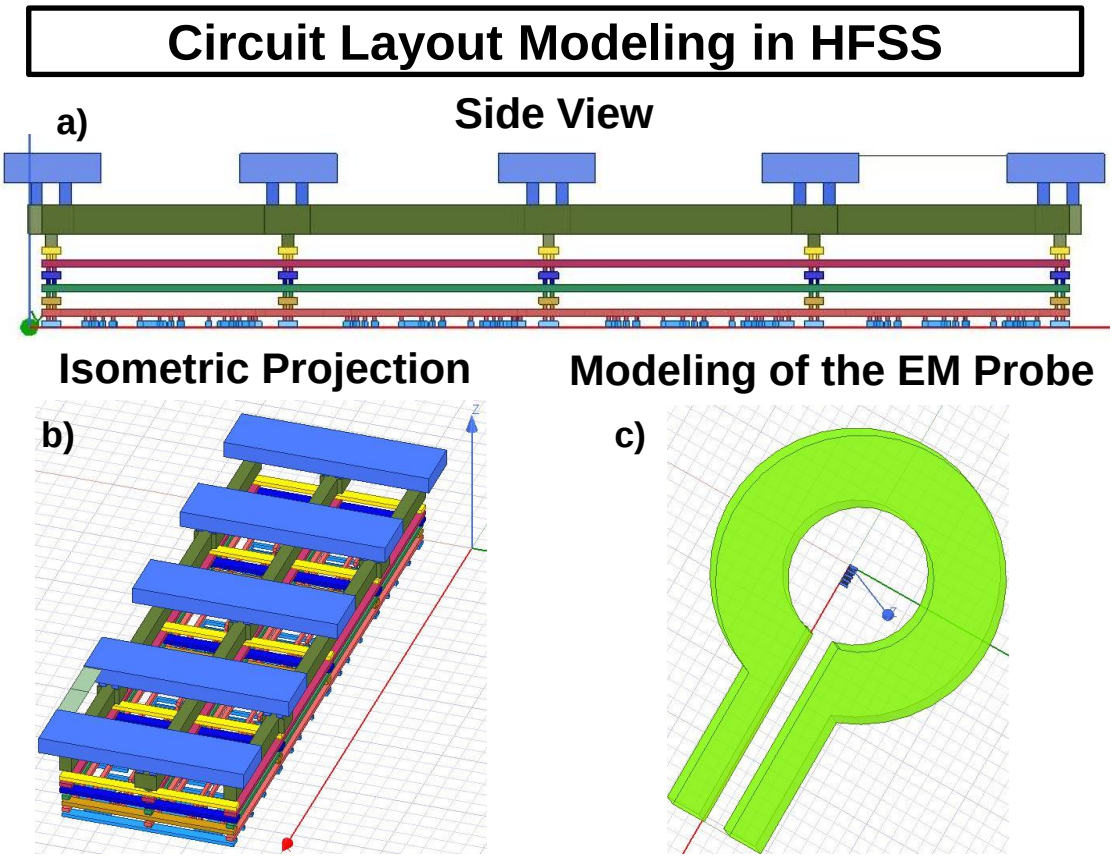


Figure 4.3. HFSS modeling: (a) side-view of a layout design, imported to and modeled in HFSS with the parameterized resistors at the bottom layer, and the voltage excitation at the top layer, (b) isometric projection of the circuit layout, (c) modeling the EM probe ($100\mu m$ loop diameter) to estimate the amount of field received across the probe at a distance of $100\mu m$ on top of the circuit under analysis (mimicking an attacker) .

limits, leading to the thermal density limits, and hence the frequency scaling in a core is restricted, moving towards multi-core designs over the last couple of decades. Hence, as we will prove later using simulations (Sec. V.C), at the operating frequencies of the CMOS circuits ($< 10GHz$), and the geometries of the metal layers involved (in μm range), the EM leakage from the circuits are in the MQS regime, which means that the EM radiation can be pre-dominantly approximated as H-field.

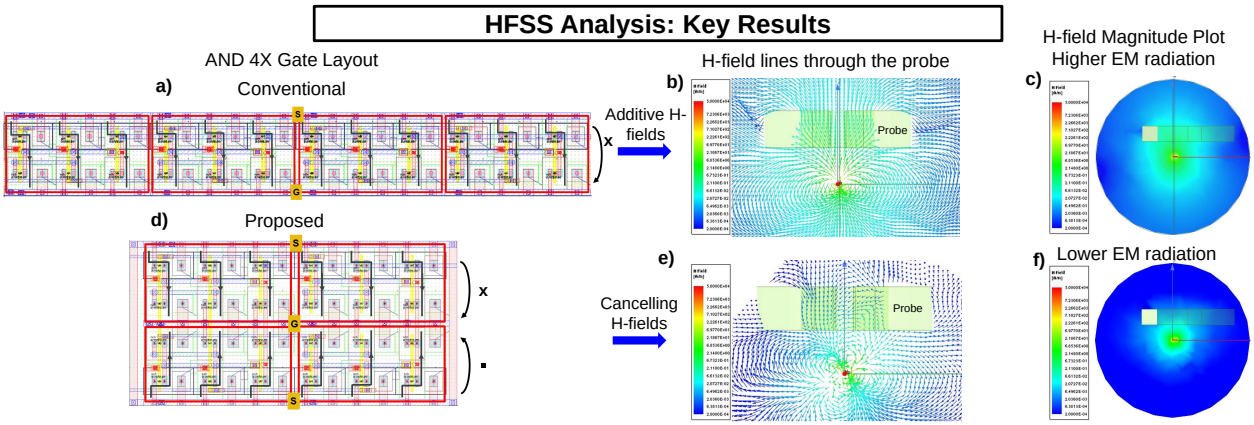


Figure 4.4. HFSS Analysis of the AND circuit for the single-row (conventional) and double-row (proposed SGS power grid): (a) conventional single-row power grid layout, (b) H-fields get added constructively and passes through the EM probe, (c) showing high EM leakage. On the other hand, (d) for the proposed double-row (SGS) power grid pattern, (e) the fields cancel out, and (f) the EM radiation is reduced drastically.

4.3.1 Reduced EM Leakage Cell Layout Design: Key Concept

Fig. 4.1(a, b) shows the key concept of the proposed digital gate layout design technique to minimize the EM leakage from an IC. Fig. 4.1(a) shows the conventional logic gate layout design which is typically seen today in the digital libraries, where the cells are placed in the same row of the power grid. Note that the same direction of current flow for all the transistors of the AND gate creates additive H-field, leading towards higher correlated EM leakage that can be picked up by an attacker.

Now, if we can somehow manage to cancel out the current flow such that the H-field is added destructively, we can minimize the EM SCA leakage picked up by an attacker. Fig. 4.1(b) shows the proposed logic gate design with the cells split across two rows of the power grid such that the alternating cell rows lead to canceling H-fields thereby minimizing the EM leakage from the source itself. As shown in Fig. 4.1, for the single-row power grid configuration, the current flow through the metal layers results in an additive H-field, while for the split double-row power grid digital gate design, the current flow results in opposing H-fields, leading to reduced EM leakage. As seen from Fig. 4.1(b), if the switching of one

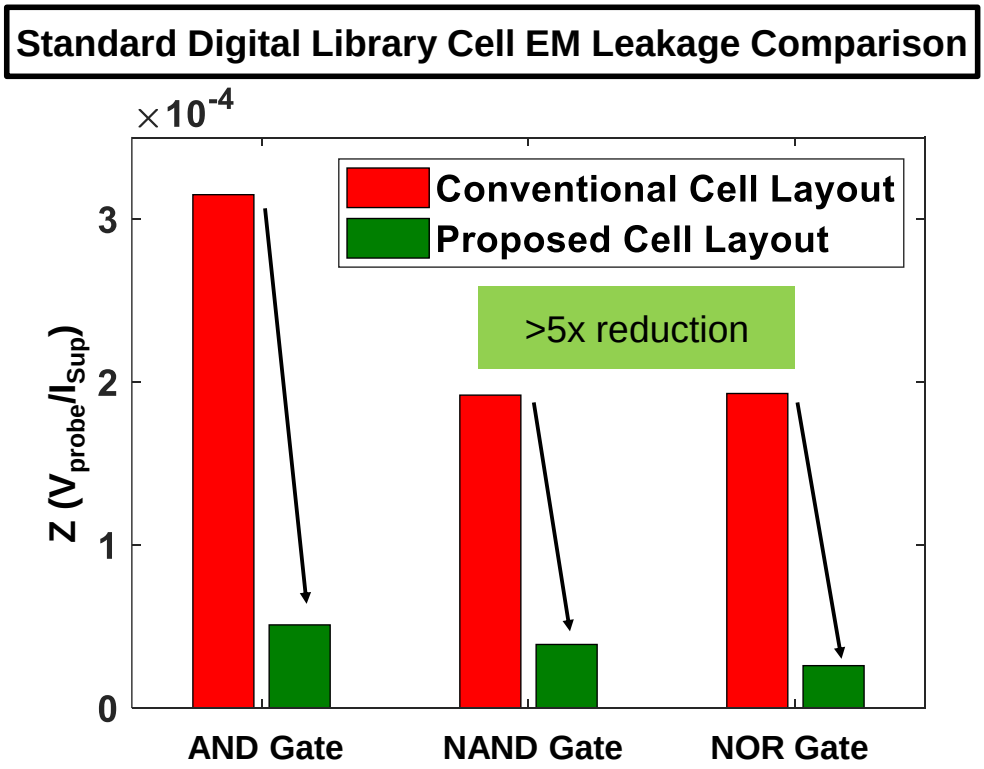


Figure 4.5. Comparison of the digital cell layout design: The y-axis shows the ratio (Z) of the voltage induced across the EM probe (V_{probe}) and the current drawn from the supply (I_{sup}). The proposed double-row SGS power grid-based layout shows $> 5\times$ reduction in the EM leakage, compared to the traditional single-row power grid-based layout across multiple different logic gates (AND, NAND, NOR) circuit analyzed.

transistor generates a clockwise current, the transistor in the adjacent row would generate an anti-clockwise current, leading to the cancellation in the H-field.

Note that for the proposed power grid configuration of the digital cells, the transistors need to be flipped in the alternate rows. This feature can be readily accommodated by today's automatic place and route (APR) tools. Fig. 4.2(a) shows the proof-of-concept AND logic gate circuit with 4X drive strength with 6 transistors. Fig. 4.2(b, c) shows the actual layout of the AND gate circuit in TSMC 65nm process in SG (supply-ground, single row) and SGS (supply-ground-supply, double row) configurations respectively. The inputs (IN1, IN2) and the output (OUT) of the AND gate are marked as shown in Fig. 4.2(a, b, c). The current flow path for the conventional AND gate (Fig. 4.2(b, c)) is marked in light

black, and the overall current flow is shown with dark black lines. In Fig. 4.2(c), for the SGS pattern, we can observe that the transistors in the two rows are flipped vertically, which ensures that the EM fields are cancelled out, in contrast to the single-row power grid layout where the EM fields get added constructively.

It is worth mentioning that, although the proposed double-row power grid layout technique does not incur any extra overheads, the only constraint it imposes is that the minimum size of the logic gates for the security-sensitive library has to be at least 2X (in our example, 4X is shown).

4.3.2 HFSS Modeling for EM Leakage Analysis

In the previous section, we proposed a double-row power grid based cell layout for minimizing the EM leakage. In this section, we will quantitatively analyze the impact of the proposed digital cell layout on the EM leakage.

Let us now investigate the EM leakage contribution from these different power grid structures implementing the same digital logic circuit with iso-area. For modeling the EM leakage from a circuit, first, we import the entire layout in HFSS and then provide the voltage excitation at the topmost metal layer (Fig. 4.3(a, b)) to emulate the powering of the chip during post-Si testing. Next, to emulate the transient currents during switching of the transistors, we insert parameterized resistors between the source and drain of the transistors. Making the parameterized resistor low resistance (short) emulates an ON transistor during the dynamic switching. Depending on the number of transistors switching at any given time, the EM leakage from the structure needs to be measured. In the later section (Sec. V), we show that only a few transistors need to be shorted, instead of all, to evaluate the EM leakage from the circuit.

Next, to analyze and compare the amount of EM leakage caused by the two different power grid layout structures, a commercially-available EM probe (Langer ICR HH100-27) with an $100\mu m$ probe loop diameter is modeled, as shown in Fig. 4.3(c). The EM probe is placed on top of the circuit layout at a height of $100\mu m$ to capture the EM radiation from the switching events occurring in the circuit. From the HFSS framework, for the amount of

current flow through the circuit (I_{sup}) depending on the number of transistors shorted at any given time, we obtain the power to EM mapping (Z), which is the ratio between the voltage received across the probe (V_{probe}) and the current drawn from the voltage source (I_{sup}).

Using this white-box modeling framework, in the next section, we will discuss the results and the effect of the different power grid configurations on the EM leakage.

4.4 Results: Effect of the Split Double-row Digital Cell Layout Design on the EM Leakage

The two iso-area layout designs (single-row SG, double-row SGS) of the same AND logic circuit ((Fig. 4.4(a, d)) are analyzed using the HFSS-based framework. Fig. 4.4(b, e) shows the H-field vector plots for the single-row SG and the double-row SGS configurations respectively, and Fig. 4.4(c, f) shows the H-field magnitude plots for the same. For the single-row (SG) digital gate layout, the field lines pass vertically through the H-probe loop (revealing an additive superposition of the field lines) and hence produces a much higher EM leakage (Fig. 4.4(b, c), light blue). On the other hand, for the proposed double-row SGS layout structure, the EM field lines cancel out as discussed in the previous section, leading to horizontal field lines which do not pass through the EM probe (Fig. 4.4(e)), leading to significantly lower EM radiation (Fig. 4.4(e, f), dark blue) compared to the traditional single-row configuration, as seen from Fig. 4.4(c, f).

To quantitatively analyze the effect of the proposed double-row power grid structure for the digital gates, the power to EM mapping or the transfer function (Z) is computed, as discussed in Sec. IV. In comparison to the conventional single-row gate layout (SG), the double-row SGS power grid provides $> 5x$ reduction in the voltage induced across the EM probe for the same amount of switching activities across all the circuits analyzed (AND, NAND, as well as NOR gates), as shown in Fig. 4.5.

Fig. 4.6(a, b) shows an extended practical use case scenario of our proposed design technique for a full-chip layout. The idea is to use the double-row split layout architecture for the critical digital gates so that the overall correlated EM leakage is greatly minimized from the source itself. However, we do not need to minimize the leakage from other uncorrelated blocks/digital cells. Hence, as shown in Fig. 4.6(b), we propose using the existing standard

digital library cells for the unrelated digital logic (other than crypto) and the double-row modified digital cell layout designs for the correlated critical digital gates to minimize the signature/signal-to-noise ratio (SNR). Further, this technique can be utilized to design the global power grid and cancel out the EM leakage even in the top metal layers.

In the next section, we will explore how our proposed framework can be extended to be used for pre-Si EM SCA evaluation prior to fabrication.

4.5 HFSS-Based Pre-Silicon EM Side-channel Evaluation

Today, the EM SCA evaluation of a crypto algorithm is mostly performed after fabrication of the chip, that is, at the post-Si phase. Hence, the countermeasures developed cannot be pro-actively tested during the design life-cycle and the designers need to wait until the chip gets fabricated, which could cost a huge amount of time and money. Hence, having a framework for evaluating the crypto implementations before fabrication is extremely critical for a faster time-to-market from an industry viewpoint. In this section, we will extend our proposed framework for the white-box analysis towards incorporating a pro-active pre-Si EM SCA evaluation within the design life-cycle of crypto ICs.

4.5.1 Limitations of the existing commercial tools

Currently, commercial tools like Cadence Virtuoso allow us to perform pre-Si power SCA evaluation. Using circuit simulators like Virtuoso, post-layout current/power traces can be extracted, but electric or magnetic fields cannot be estimated. On the other hand, Ansys HFSS and Redhawk (static IR-drop simulator) are used for EM analysis, and are popularly utilized for inductor or antenna design. However, HFSS or Redhawk cannot be used to simulate an entire circuit layout as it involves huge complexity. In this work, by identifying what precisely needs to be simulated in HFSS (unlike the prior works [93], [116]), we combine both the commercially-validated tools, Virtuoso and HFSS together, to obtain the EM traces and perform the pre-silicon EM side-channel analysis on any crypto algorithm (Fig. 4.7).

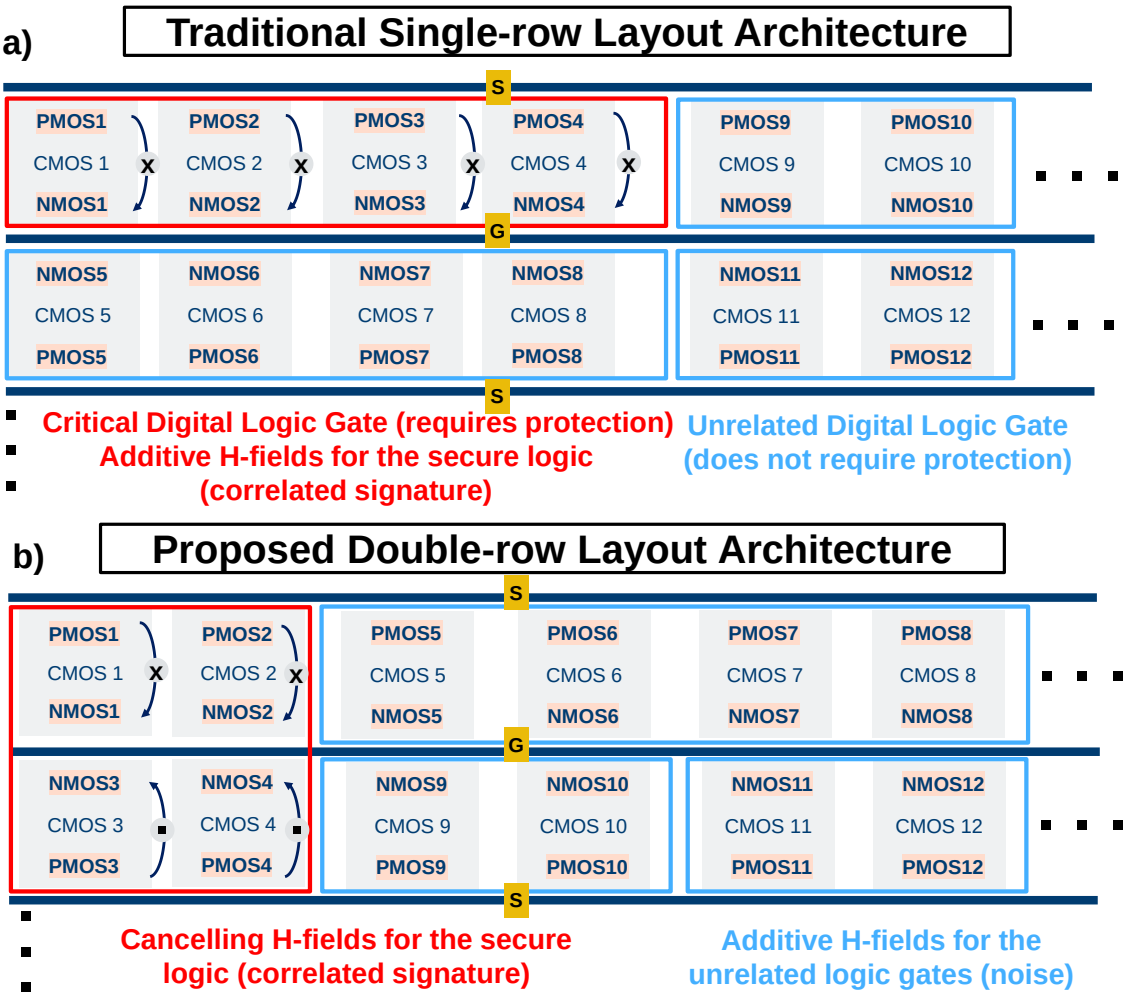


Figure 4.6. (a, b) Practical use case of the proposed digital cell layout architecture for a full-chip layout. The proposed double-row power grid layout cell should be used for the security-critical digital logic to reduce the correlated EM leakage, while the traditional single-row gate layouts are used for unrelated logic (other than crypto), which do not require side-channel protection to enhance the uncorrelated EM leakage (increase system noise), so that the signal-to-noise ratio (SNR) of the EM measurements is reduced drastically for an attacker.

4.5.2 EM SCA Pre-Si Evaluation Framework: Key Concept

As shown in Fig. 4.7, the first step in building this framework for pre-Si EM SCA evaluation is to obtain the simulated post-layout current/power traces. Secondly, the layout of the circuit is modeled in HFSS and the power to EM mapping (Z) is obtained (Sec. III),

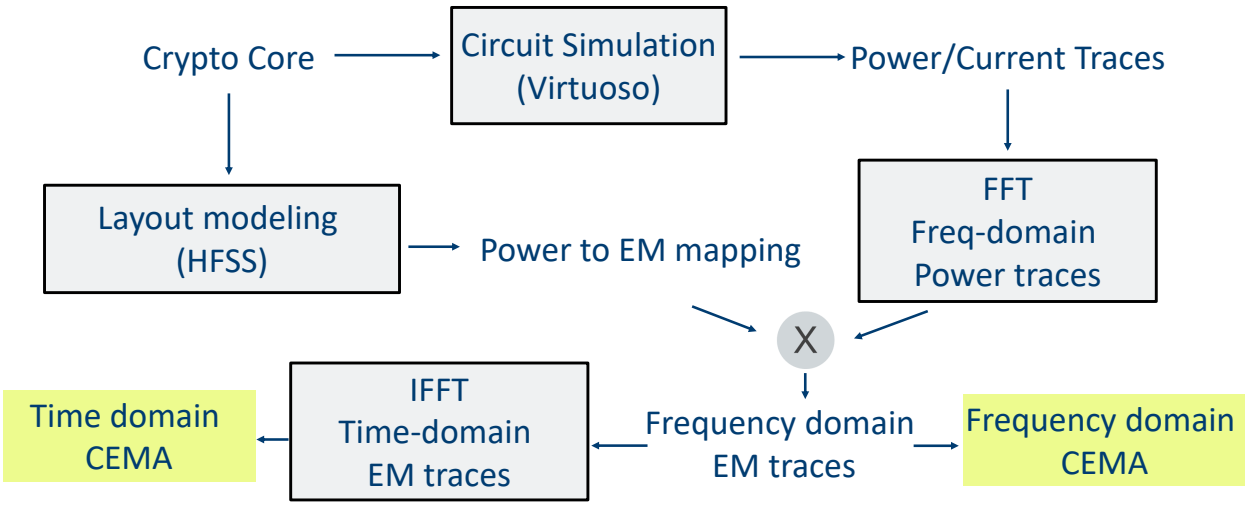


Figure 4.7. Flowchart of the pre-Si EM SCA evaluation framework.

specific to the circuit layout, across different frequencies. Thirdly, the time-domain power traces are transformed into the frequency-domain through fast fourier transform (FFT). This transformation to the frequency domain is performed for our convenience as we shall see in the next sub-section. Now, this power to EM mapping is applied on the frequency-domain current traces to compute the corresponding frequency-domain EM traces (refer to Fig. 4.7). Finally, a frequency-domain CEMA is performed on the synthesized frequency-domain EM traces. Alternatively, the frequency-domain EM traces could also be transformed into time-domain and then the conventional time-domain CEMA can be performed to extract the secret key and evaluate the resiliency of the crypto system in the pre-Si environment.

4.5.3 Power to EM Transfer function & Frequency response

The power to EM transfer function (Z) for a 16:8 MUX circuit is shown in Fig. 4.8(a, b) as a proof-of-concept. Fig. 4.8(a) shows the voltage induced across the EM probe (V_{probe}) and the current drawn from the supply (I_{sup}) as a function of the number of transistors switching in the circuit. Fig. 4.8(b) shows the power to EM mapping (Z) which is the ratio of the V_{probe} and I_{sup}. We can clearly see that the transfer function remains independent of the number of switching events at the operating frequency of 1GHz. This is as expected, since the amount of current drawn from the supply (I_{sup}) and the voltage induced across

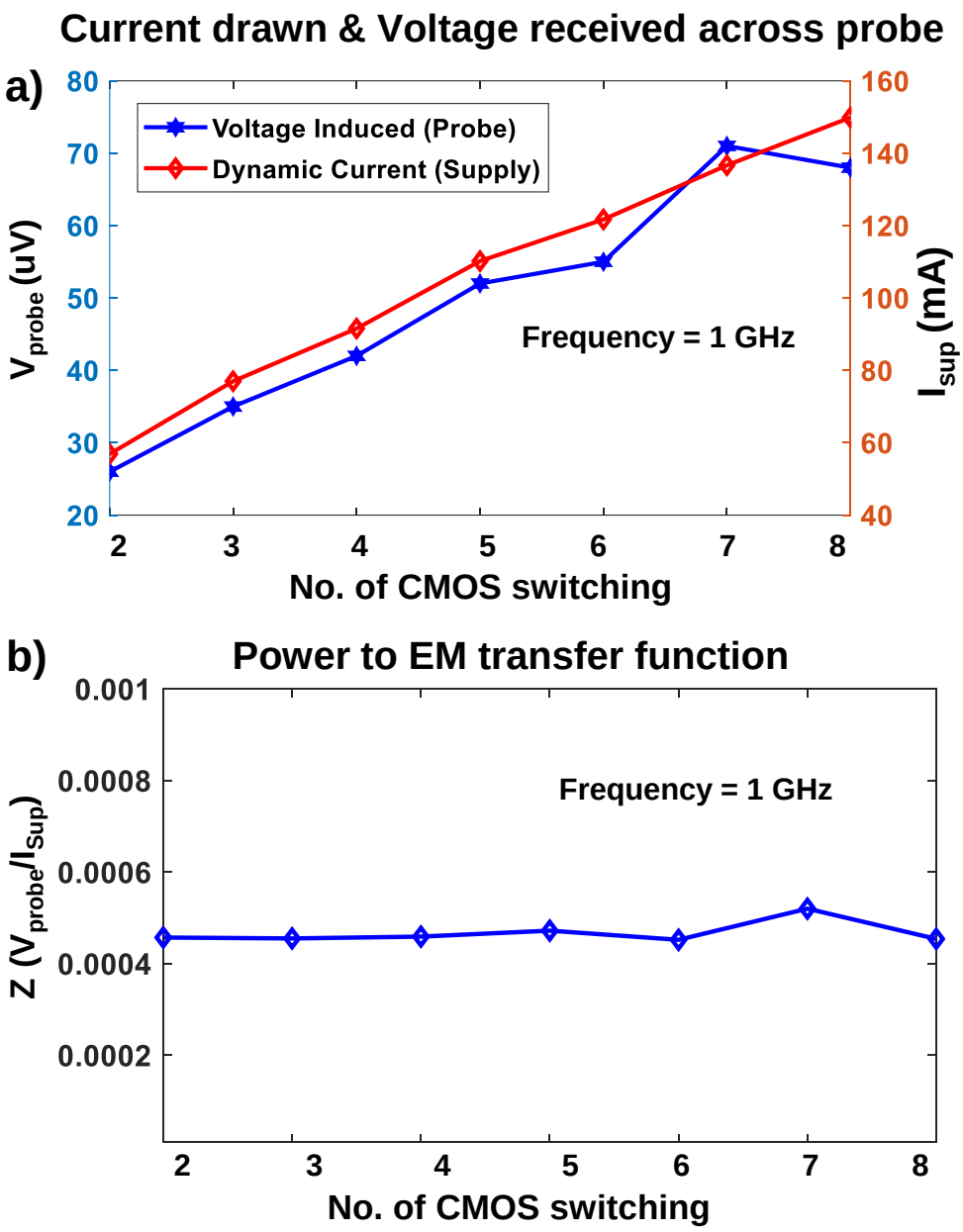


Figure 4.8. Power to EM mapping: (a) The voltage induced across the EM probe (V_{probe}) and the current drawn from the supply (I_{sup}) for different number of CMOS switching events for a 16:8 MUX circuit is analyzed as a proof-of-concept. (b) The power to EM mapping/transfer function (Z) is independent of the number of switching events in the circuit.

the EM probe (V_{probe}) should remain linear at low frequencies. This is an important result and the key take-away is that **the power to EM mapping for a given circuit is now**

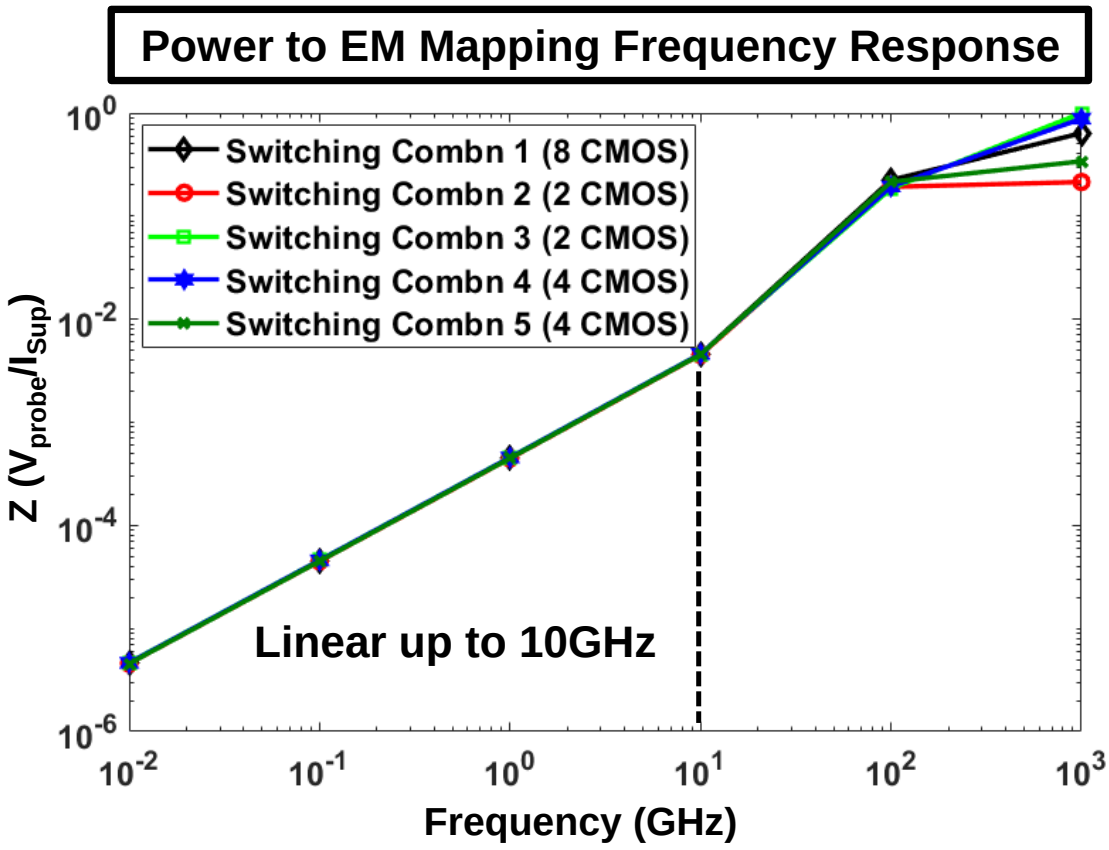


Figure 4.9. Power to EM transfer function (Z) frequency response: Z remains linear with frequency up to $\sim 10GHz$, revealing the MQS mode of operation. Also, for the different transistor switching combinations, the mapping remains the same (as we see the curves are overlapping till $\sim 100GHz$).

possible by only shorting a few transistors instead of all, making it easier to scale across larger circuits.

Now, as seen in Fig. 4.9, the transfer function (Z) remains constant (curves overlap) for all the different transistor switching patterns, and the mapping remains linear across different frequencies up to 10GHz. Most of today's embedded devices operate below this frequency limit, and frequency scaling in a core is limited due to the energy constraints and the thermal density, leading towards multi-core architectures since the last couple of decades. Hence, the important take-away from this result is that the power to EM mapping (Z) scales linearly with frequency, which is consistent with Biot Savart's Law, proving the magneto-quasistatic (MQS) approximation at the low frequency range. Note that, the metal

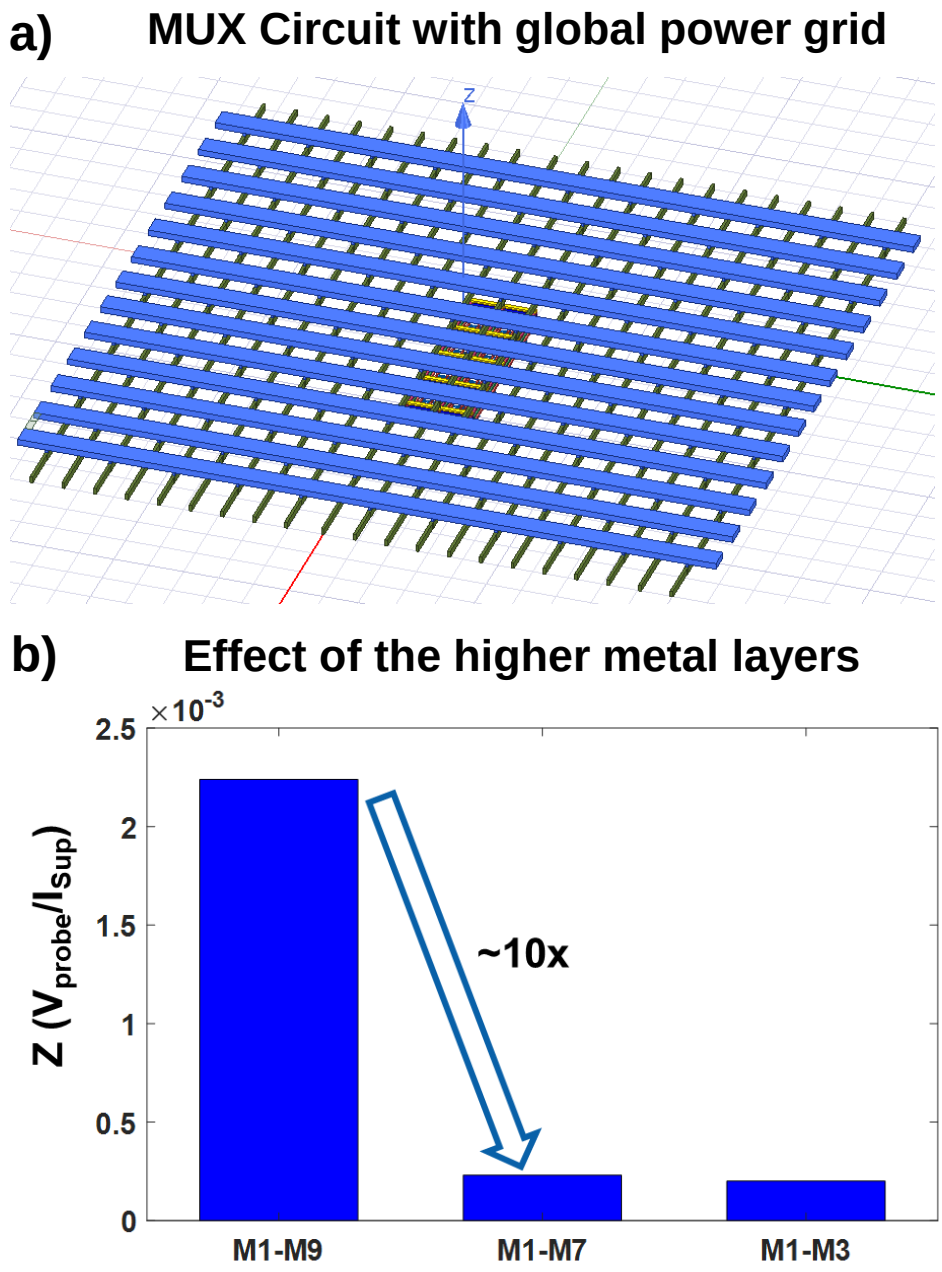


Figure 4.10. Effect of the higher metal layers is demonstrated. (a) The MUX circuit is designed with the global power grid, emulating the global supply and ground for the entire IC (instead of just the local circuit under analysis). (b) These top metal layers (M8, M9 for the TSMC 65nm technology), which forms the global power grid contribute significantly to the EM leakage compared to the lower metal layers, re-validating the prior works [43], [37].

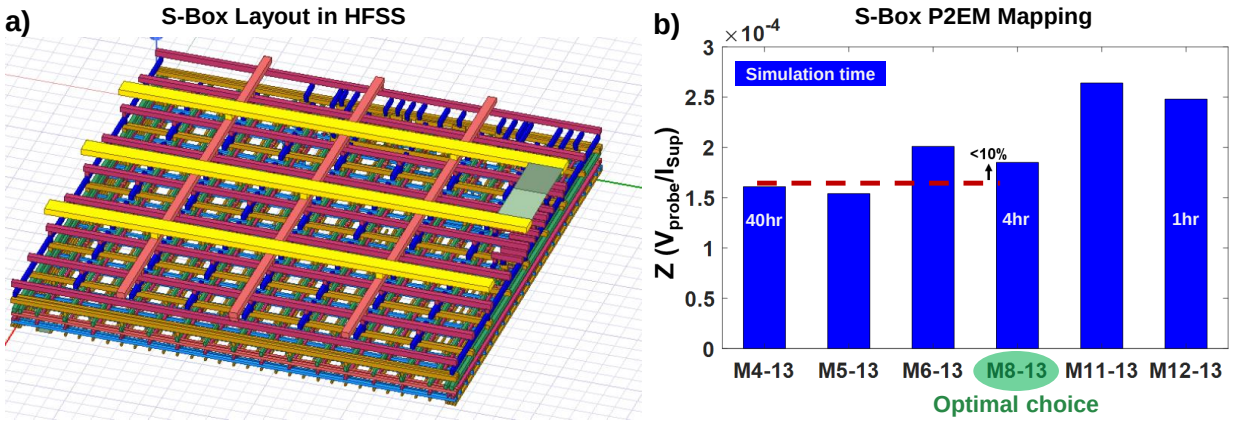


Figure 4.11. S-Box power to EM mapping: (a) S-Box layout and its 3D modeling in HFSS; (b) the power to EM mapping for S-Box circuit.

layers have resonant peaks at the THz frequency range, but we are only concerned below 10GHz, where the transfer function remains linear with frequency. This is the main reason why the power to EM mapping is performed in the frequency domain as it would alleviate the need for measuring the transfer function Z across all the frequencies (utilizing the linear mapping).

4.5.4 Scalability to real crypto implementations: Elimination of the lower metal layers

Till now, in this section we have analyzed the 16:8 MUX circuit with only $\sim$ 50 transistors. However, real-world crypto primitives like the S-Box or a full AES would have 1000$\times$ more transistors. Modeling the full circuit in HFSS is complicated as it cannot be handled by the graphics support. As of early 2021, even a powerful machine with 16 cores, 100 GB RAM was unable to load the S-Box circuit fully, due to graphics limitations (most likely owing to the millions of small dimension metals in the lower layers).

Now, it is known from prior works [37] that the higher metal layers of an integrated circuit contributes the most to the EM leakage, due to its higher thickness and longer length of routing (global power grid). Hence, as seen in Fig. 4.10(a, b), modeling the MUX circuit with the global power grid on the top two metal layers, the effect of the higher-level metal layers is re-validated (with previous work [37]) since removing just the top two metals reduces

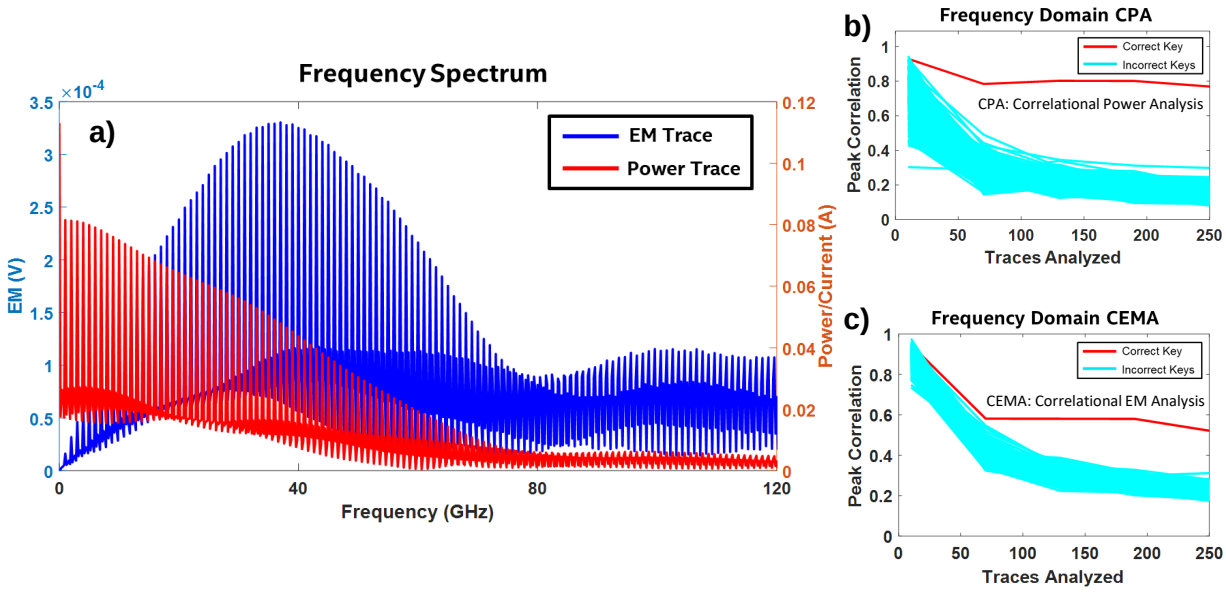


Figure 4.12. S-Box CEMA: (a) Frequency spectrum of the power traces (red curve) and the transformed EM traces (blue curve) using our proposed framework. (b) Frequency-domain CPA shows the correct key separating out in $\sim$ 10 traces, while (c) CEMA attack shows the correct key extracted in $\sim$ 50 traces, validating the proposed pre-Si EM side-channel evaluation framework.

the EM leakage drastically by $\sim 10\times$. Now, with this understanding that the higher metal layers are the main contributors of the EM leakage, we can remove some of the bottom metal layers and obtain the power to EM mapping (Z). This would help scale to larger circuits like the S-Box or even an AES.

4.5.5 Results: S-Box CEMA

For scaling towards larger circuits, we consider a S-box implementation, which is a security primitive for symmetric key algorithms like AES. This application-based study has been performed in the Intel 10nm process (Fig. 4.11), which has 13 metal layers (M1-M13) [122]. The layout of the S-Box is generated using the commercial automatic place and route (APR) tools. As discussed earlier, the higher metal layers contribute significantly more to the EM SCA leakage compared to the lower metal layers, and hence we model the S-box layout in HFSS (Fig. 4.11(a)), starting from metal layer 4 (M4) and then removing one layer at a time to determine the optimum point for the power to EM mapping (Z) for this particular

technology. As seen from Fig. 4.11(b), as we remove one layer at a time, the simulation time reduces drastically, while the accuracy of the power to EM mapping (Z) also reduces. Analyzing the layout structure, we observe that the power to EM mapping starting from metal layer M8 going up to metal M13 is the most optimal choice in terms of the simulation time and accuracy for this particular technology (Intel 10nm).

As discussed earlier, it is not feasible to simulate a large circuit with the entire metal stack due to its sheer complexity with all the transistors (and numerous tiny metal-via structures) at the lowest layer. Hence, the optimal choice of simulation from M8-M13 (for the Intel 10nm process) simplifies the flow and allows us to form an estimate of the EM SCA leakage in pre-Si environment, which is critical to evaluate the efficacy of a crypto engine and its countermeasure, prior to fabrication.

Note that, the power to EM mapping is only required to be computed at one frequency of interest (1 GHz, for our case), as it can be linearly scaled across other frequencies (Fig. 4.9), as evidenced by the MQS region of operation at these low frequencies and the geometry of the radiating elements, that is, the IC metal layer dimensions. Now, once the power to EM mapping (Z) is obtained from our HFSS model, we simultaneously simulate the S-box circuit using Virtuoso to obtain the power traces in the time-domain. The power traces are transformed to the frequency domain using FFT (Fig. 4.12(a), red curve), and the power to EM transfer function (Z) is applied on the power traces to obtain the corresponding EM traces in the frequency domain (Fig. 4.12(b), blue curve). Now, we perform a correlational power analysis (CPA) on the frequency-domain power traces using the hamming weight model as shown in Fig. 4.12(b) which reveals the correct key in $\sim$ 10 traces. CEMA is performed on the transformed frequency-domain EM traces which also successfully reveals the correct key in $\sim$ 50 traces, validating the proposed HFSS-based framework. Similarly, the CEMA can also be performed in the time domain after transforming the generated frequency domain EM traces to the time domain through inverse FFT (IFFT), as discussed earlier (Sec. V.C, Fig. 4.7). The minimum traces to disclosure (MTD) is low since the noise is not added to the system, which can be modeled independently based on the system under consideration.

4.6 Conclusion & Future Work

To summarize, this work developed a framework to perform white-box modeling of the EM leakage from a crypto IC and proposed a new digital gate layout architecture to minimize the EM leakage. Using the HFSS-based framework, it was demonstrated that the double-row power grid layout pattern (supply-ground-supply (SGS)) for digital logic gates has significantly lower leakage compared to the traditional single-row layout pattern (supply-ground (SG)). This is a generic technique, which is agnostic of any crypto algorithms and does not incur any overheads. For practical large design layouts, we proposed using the traditional standard library cells for the unrelated digital logic gates (other than crypto), while the proposed double-row-based modified digital gate layouts for the security-critical logic to minimize the SNR significantly and thereby prevent EM SCA attacks.

The HFSS-based framework is extended to develop a pre-Si EM SCA evaluation technique combining both Virtuoso and HFSS. Hence, CEMA can now be performed during the design phase itself, which is extremely useful to evaluate the crypto implementations and countermeasures before a chip is fabricated, thereby reducing the time to market drastically for security sensitive designs.

In the next chapter, we will look into the side-channel countermeasures and deep-dive into the circuit-level implementation of a generic low-overhead EM/power SCA resilient AES256 design in TSMC 65nm CMOS technology.

5. EM & POWER RESILIENT AES-256 IN 65NM CMOS THROUGH CURRENT DOMAIN SIGNATURE ATTENUATION & LOCAL LOWER METAL ROUTING

Most of the materials in this chapter have been extracted verbatim from the paper:
1. Debayan Das et al., EM and Power SCA-resilient AES-256 in 65nm CMOS through $> 350\times$ Current Domain Signature Attenuation & Local Lower Metal Routing, *IEEE Journal of Solid-State Circuits (JSSC)*, 2021.

Mathematically secure cryptographic algorithms, when implemented on a physical substrate, leak critical 'side-channel' information leading to power and electromagnetic (EM) analysis attacks. Circuit-level protections involve switched-capacitor, buck converter, or series low dropout regulator (LDO) based implementations, each of which suffers from significant power, area or performance trade-offs and has only achieved a minimum traces to disclosure (MTD) of $10M$ till date. Utilizing an in-depth white-box model, this work for the first time focuses on signature suppression in the current domain which provides an $Attenuation^2$ enhancement in MTD leading to orders of magnitude improvement in both power and EM side-channel analysis (SCA) immunity. Using a combination of (1) current-domain 'signature attenuation' (*CDSA*) along with (2) local lower-level metal routing, the critical correlated information in the crypto current is significantly suppressed before it reaches the supply pin. Specifically, to prevent the EM leakage from its source (metal layers carrying the correlated crypto current acting as antennas), this work embraces lower-level metal routing of the *CDSA* embedding the crypto IP, so that the signature becomes highly suppressed before it passes through the higher metal layers (which radiates significantly) to connect to the external pin. The 65nm CMOS test chip contains both protected and unprotected parallel AES-256 implementations, running at a clock frequency of 50MHz. Test vector leakage assessment (TVLA) on the protected *CDSA-AES*, demonstrated with on-chip measurements for the first time, show that the higher-level metal layers leak significantly more compared to the lower-level metal routing. Correlational power and EM analysis (CPA/CEMA) attacks on the unprotected implementation were able to extract the

secret key within $8k$ and $12k$ traces respectively, while the protected *CDSA-AES* could not be broken even after $1B$ encryptions for both power and EM SCA, evaluated both in time as well as frequency domain, showing an improvement of 100× over the prior state-of-the-art countermeasures with comparable power and area overheads.

5.1 Background

5.1.1 Motivation

Recently, AES-256 was shown to be broken in 5 minutes from a 1 meter distance (and within few seconds from 30 cm away) using non-invasive EM probes [123]. The time-complexity of breaking an AES-256 is reduced from 2^{256} for brute-force attacks to 2^{13} for SCA attacks. Transitioning from AES-128 to AES-256 increases the mathematical security exponentially, however the SCA security only increases linearly by 2×.

For performing an EM/power SCA attack, first, the EM/power traces are measured from the crypto engine using an oscilloscope or a high-resolution analog-to-digital converter (ADC). Next a hamming weight (HW) or hamming distance (HD) model is built for different key guesses depending on the point of attack. Finally, correlation is performed between the collected traces (T) and the attack model (H), and the correct key showing the highest correlation emerges out after multiple traces are analyzed. These correlational attacks (CEMA/CPA) do not require any prior timing information on the occurrence of the targeted operation, since the correlation coefficient ρ_{TH} can be calculated at each time sample of the EM/power trace [71].

A HW-based attack is often effective for software crypto implementations running on a microcontroller, while HD attacks are more prominent on efficient hardware implementations as operations are more parallelized. Also, the point of attack on a crypto algorithm may change from software to hardware implementations. For instance, in the case of software AES-256, the output of the 1^{st} round S-box can be targeted to derive the key using chosen plaintexts (PT). However, for hardware implementations, attacking combinational logic is not easy (due to the different delays for different inputs). Hence, in case of a hardware AES-256 parallel datapath implementation, a known ciphertext (CT)-based attack on the HD for

the last 2 rounds (13^{th} and 14^{th}) is more effective and practical, and has been adopted for this work to evaluate the resiliency of both the unprotected and protected versions of the AES-256.

Real-world examples of EM/power SCA attacks include counterfeiting e-cigarette batteries by stealing the fixed secret key embedded in the authentic device to gain market share. Also, recently, SCA attacks on bitcoin wallets were demonstrated to recover the private key. In general, these attacks can be used to obtain the secret key from the boot-loader of any embedded device [85].

As the attacks are constantly improving and attackers are becoming even more powerful with the advent of better EM probes, it is imperative that we devise ***energy-efficient generic techniques*** to protect against both EM/power SCA attacks for any crypto algorithm. **Circuit-level on-chip countermeasures** include switched capacitor current equalizer [106], charge recovery logic [124], IVR [125], and all-digital LDO [120], which suffer from performance degradation, high power and area overheads because of large embedded passives, as well as EM leakage from large MIM capacitor top plates.

5.1.2 Key Concepts

In this work, aided by the white-box analysis of the EM leakage from a crypto IC, we strive to tackle the problem of EM leakage at its source [40]. Fig. 5.1(a, b) shows the overview of the proposed current domain signature attenuation (CDSA) countermeasure, which provides a significant signature suppression such that the MTD is improved by a factor of $Attenuation^2$ (AT^2) [37]. It should be noted that in the security/side-channel community, SNR is defined as the ratio of the variances of the power/EM trace and the noise, while in our work, SNR is considered as the ratio of the voltages, as defined within the circuits community (Fig. 5.1(a)). The lower-level metal routing of the CDSA embedding the crypto core ensures that only the suppressed critical signature passes through the higher metal layers, thereby simultaneously protecting against both power as well as the EM SCA attacks. This will be discussed in detail in Section III.

The key concepts of this chapter are summarized as follows:

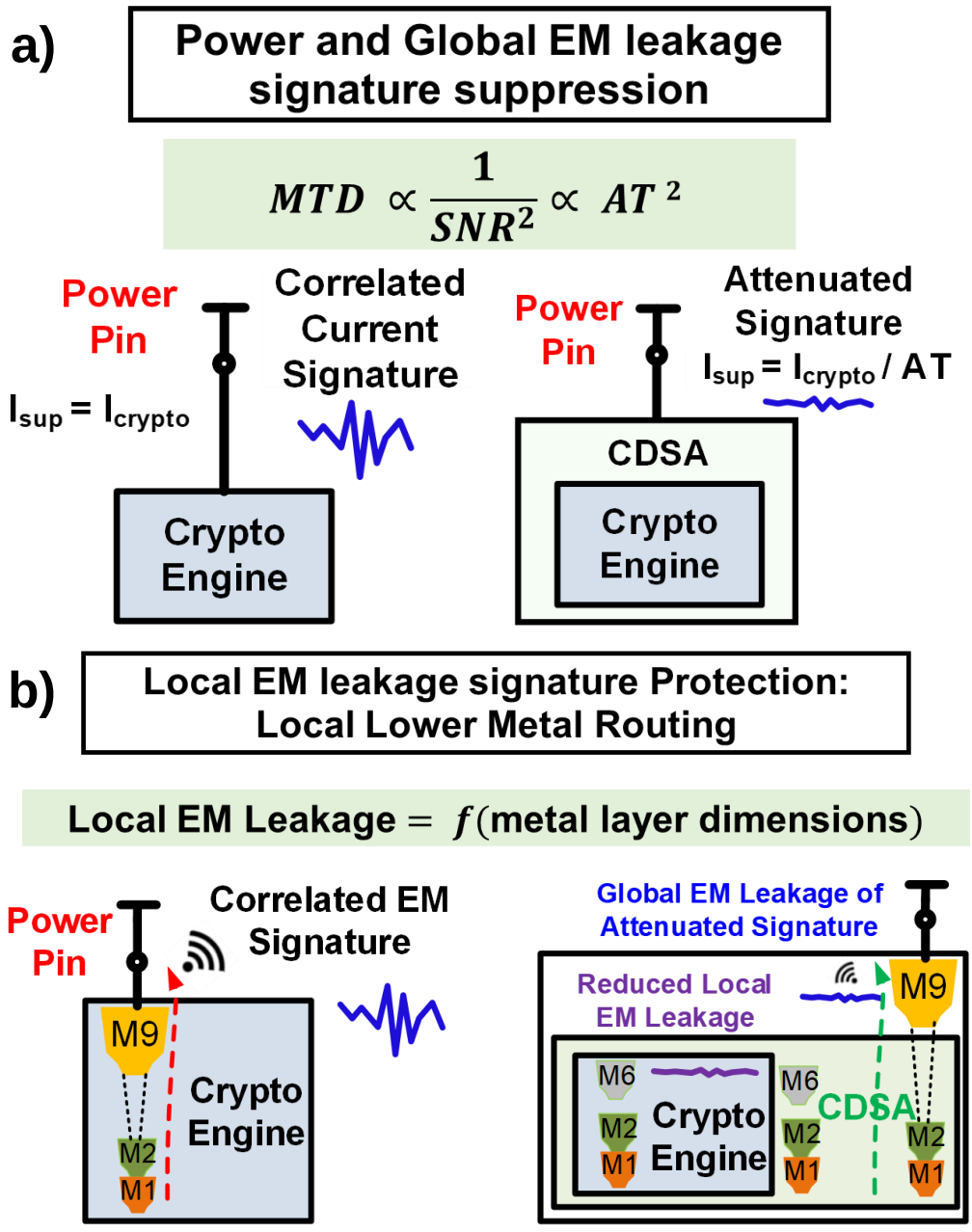


Figure 5.1. Overview of the CDSA Design Techniques: (a) Inline current domain signature attenuation fundamentally reduces the correlated crypto current information and provides orders of magnitude improvement in the SCA security for both power as well as the global EM leakage. (b) Local lower-level metal routing of the CDSA embedding the crypto core enables a local EM signature suppression such that the EM radiation from the higher level metal layers do not leak the critical information.

- **Current-domain signature attenuation** (*CDSA*) technique ensures that the correlated crypto current is significantly suppressed before it reaches the supply pin, providing an $Attenuation^2$ (AT^2) improvement in the SCA security of cryptographic devices. It thereby provides resilience against both *power as well as the 'global' EM leakage*.

- **Local lower metal routing** technique helps in reducing the *local EM SCA leakage*. The idea is to suppress the critical correlated crypto signature within the lower-level metal layers (up to M_6 in our case) before it goes through the higher metals (root-cause of the EM leakage) to connect to the external pin. Also, the CDSA hardware embedding the crypto core in the lower metals has to be 'local' to minimize the IR drop.

The fabricated 65nm CMOS test chip contains both the unprotected and protected implementations of AES-256, which are subjected to CPA and CEMA attacks, showing that the unprotected AES can be broken in only $8k$ and $12k$ traces respectively, while the *CDSA-AES* remains protected even after $1B$ traces, achieving 100× higher minimum traces to disclosure ($MTD > 1B$) reported to date with comparable power and area overheads.

Additionally, this work, for the first time, demonstrates the effect of metal layers on the EM side-channel leakage. Using test vector leakage assessment (TVLA) methodology, it can be seen that the *CDSA-AES* with higher level metal routing leaks significantly more ($> 7\times$) compared to lower-level metal routing, proving the effects of on-chip metal layers on EM leakage.

5.2 Related Works

Power and EM SCA countermeasures can be broadly classified into 3 categories: logical, architectural and physical. **Logical** countermeasures focus on equalizing the power consumption in each clock cycle and include sense-amplifier based logic (SABL) [102], dual-rail precharge circuits [103], wave dynamic differential logic (WDDL) [104], and gate-level masking [126], [96]. These countermeasures usually require re-designing the library cells and also suffer from high area and power overheads as the logic gates are replaced with a sophisticated one to mask the side-channel leakage.

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	-

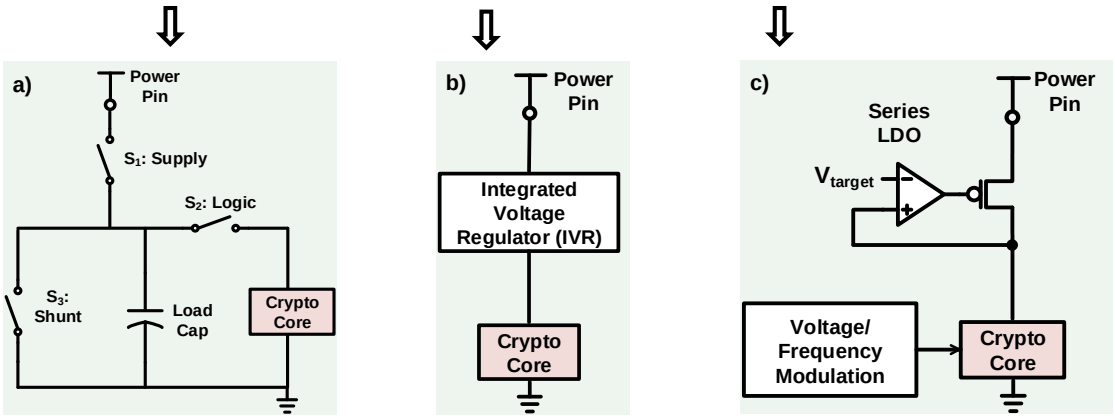


Figure 5.2. State-of-the-Art Circuit-level Countermeasures: (a) Switched Capacitor Current Equalizer [10], (b) Integrated voltage regulator (IVR) using buck converter with loop randomization [12], (c) Digital low-dropout (LDO) regulator with clock modulation [13]. The table on the top highlights the main challenges with the existing implementations. In the upcoming sections, we will see how we can achieve an MTD of $1B$ even with a much smaller load capacitor (150pF), thereby reducing the area overheads.

The second category involves **architectural** countermeasures based on introducing time or amplitude based distortions using dummy insertion, or shuffling of operations, which provide limited enhancement in SCA security depending on the algorithm and architecture of the implementation [127].

The third and final category include the physical **circuit-level** countermeasures to protect against EM and power SCA attacks. These are the most generic techniques, and involves noise injection, switched capacitor based current equalizer [106],[128], integrated voltage regulator (IVR) using buck converters [125], and digital LDO based implementation [120]. Simulations of shunt LDO based regulators have been recently studied and shown to be effective for power SCA resistance [42]. Noise injection based countermeasure reduces the signal-to-noise ratio (SNR), but suffers from very high power overheads and hence is not an optimum technique to enhance SCA security [41].

Switched capacitor current equalizer circuit proposed by Tokunaga et al. [106] operates in three phases, as shown in Fig. 5.2(a). In the first phase (S_1 closed), the load capacitor is charged to supply. The AES core operates in the second phase (S_2 closed) and finally in the third phase (S_3 closed), the load capacitor is discharged to a fixed bias to clear the voltage residue. Although this is a novel supply isolation technique, it has multiple trade-offs among the size of the load capacitor (performance vs. area trade-off), the dc bias voltage (security vs. power trade-off), as well as the switching frequency (area vs. power trade-off), leading to a 2× performance degradation.

Integrated voltage regulator (IVR) using buck converter along with loop randomization was proposed in [125] as shown in Fig. 5.2(b). However, it suffers from large passives including on-board inductors, as shown in the table in Fig. 5.2.

Recently, as shown in Fig. 5.2(c), series LDOs with noise injection along with voltage frequency modulation was proposed to obfuscate the side-channel leakage [120]. However, it used large MIM capacitors which can leak the critical side-channel information through the higher-level metal layers in the form of EM leakage. Also, ideal series LDO-based implementation inherently leaks critical information [42], as it tries to maintain a constant voltage across the crypto core which means that the current drawn from the supply is exactly equal to the crypto current, which is undesirable for SCA resistance.

In this work, the goal is to achieve a high MTD with lower load capacitor. By adopting the two key design techniques (refer to Section II. B), the proposed CDSA design achieves both EM as well as power SCA protection up to an MTD of $1B$ traces, thereby improving the state-of-the-art by 100×, with a 10× lower load capacitance.

5.3 Global Signature Attenuation: Concept & Circuit Design

In this section, we will study the details of the the CDSA countermeasure to protect against power as well as the global EM side-channel leakage.

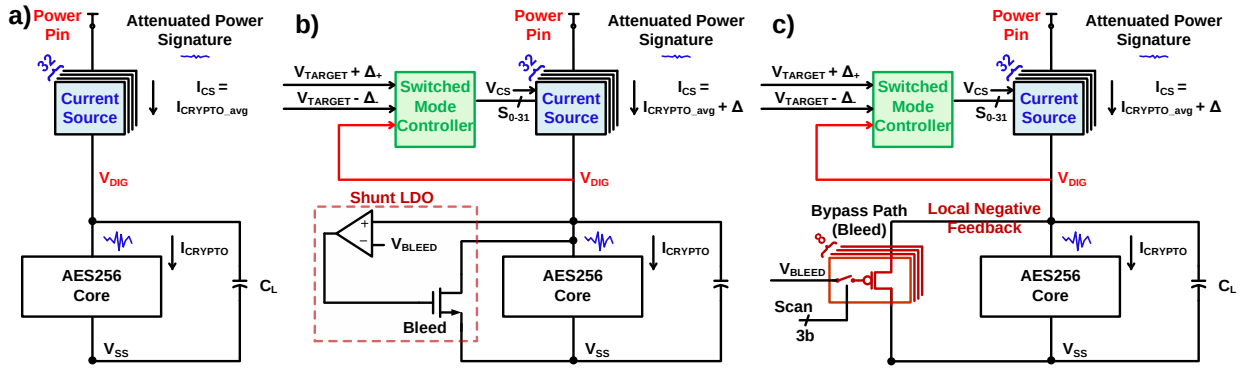


Figure 5.3. Build-up to the CDSA Design: (a) Ideal realization of a current source, (b) Low Bandwidth Switched Mode Controller (SMC) for PVT tolerance and choosing the number of CS slices for supplying the average AES current, and the high bandwidth shunt LDO to bypass any extra current from the top that is more than the average current of the AES-256 core. (c) The shunt LDO is replaced with a PMOS bleed transistor which provides an inherent negative feedback as well as the low frequency regulation with much lower power and still providing the same SCA security benefits.

5.3.1 Concept

For an unprotected crypto engine, the supply current remains equal to the crypto current as shown in Fig. 5.1(a). Our goal is to design a countermeasure such that the supply current is independent of the crypto current.

Imagine if we can somehow embed the crypto core within a current-domain signature attenuation (CDSA) hardware such that the correlated current signature is significantly suppressed (almost constant) even before it reaches the supply pin, then the MTD for power SCA would be enhanced by the square of the attenuation factor ($MTD \propto AT^2$), as shown in Fig. 5.1(a). The MTD for EM SCA is also improved as the current flowing through higher-level radiating structures (e.g. pins, board traces) is near constant. This idea of suppressing the signature in the current domain provides huge benefit in terms of SCA security for both power as well as the global EM leakage.

5.3.2 Circuit Architecture

For designing a current-domain signature attenuation (CDSA) hardware, we need the supply current to be independent of any variations in the crypto current. The first thing that comes to our mind is a constant current source (CS). However, a constant CS cannot drive a variable current load. Hence, we need a capacitor to account for the differences in the current, as shown in Fig. 5.3(a).

Now, as shown in Fig. 5.3(b), to handle the PVT variations, a low bandwidth switched mode control (SMC) loop is used which tracks the V_{DIG} within a guard band of $V_{TARGET}+\Delta_{+}$ and $V_{TARGET}-\Delta_{-}$ by turning ON or OFF the required number of CS slices [129], [130], [131]. The SMC loop thus tries to set the CS current to the average crypto current. However, due to the quantization levels of the CS, the supply current (I_{CS}) is set to the the closest higher quantization level ($I_{CRYPTO_{avg}}+\Delta$).

Now, to drain the excess current (Δ), a high power shunt LDO [132], [129], [42] can be utilized which senses the node V_{DIG} and controls the bleed NMOS gate voltage to draw the difference of current between I_{CS} and I_{CRYPTO}. However, the shunt loop needs to be very high bandwidth ($\sim 10\times$ more than the crypto frequency) to respond to the instantaneous changes in the load (crypto) current, and hence would incur a high power overhead. Instead, as shown in Fig. 5.3(c), a PMOS bleed path is designed which provides a bypass path for the extra current (Δ) and minimizes the power overhead significantly.

5.3.3 Cascode Current Source: Lower Load Capacitor

To achieve high signature attenuation (AT), we need a high output impedance CS or a high load capacitor. Hence, a cascode CS is chosen as shown in Fig. 5.4(a) which provides a high output impedance (r_{ds}) compared to one-stack CS, and allows $10\times$ lower load capacitor (C_L) to achieve iso-attenuation as shown in Fig. 5.4(b). The CDSA utilizes digitally-tunable cascode current source (CS) with high output impedance to power the AES. Although the choice of a smaller load capacitor (C_L) leads to voltage fluctuations ($\sim 30-50mV$) at the V_{DIG} node (Fig. 5.4(c)), the high output impedance of the CS stage ensures that the voltage fluctuations are not reflected to the supply current which an attacker can access.

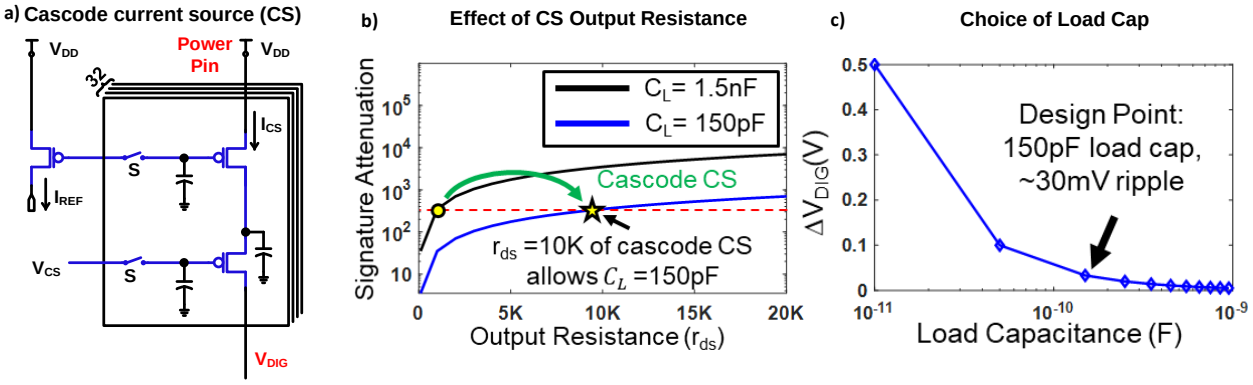


Figure 5.4. Design of the Constant Current Source: (a) A cascode current source provides (b) 10× higher output impedance compared to a simple current source implementation, (c) and hence allows a 10× reduction in the load capacitor for iso-attenuation.

5.3.4 CDSA Design

As discussed in Section II, traditional LDOs inherently leak critical information [42]. For the CDSA design, the supply current does not track the AES current, and hence the SMC loop is a low-bandwidth control loop to set the supply current to the average crypto current. Instead, we choose to tolerate the $\sim 30 - 50mV$ voltage droop across the AES engine, and the high impedance ($r_{ds} > 10K\Omega$) CS on top ensures that the current fluctuation at the supply is attenuated by,

$$AT = \omega_{AES} C_L r_{ds} \tag{5.1}$$

which evaluates to $> 350\times$.

The goal of the CDSA circuit is to provide the average load (AES) current plus a delta current that leaks through the bypass PMOS bleed path to ground, providing local negative feedback which leads to the ability to support any $I_{AES_{avg}}$ in between two quantized current levels of the CS. Hence, the shunt-path PMOS bleed (biased for near-threshold operation)

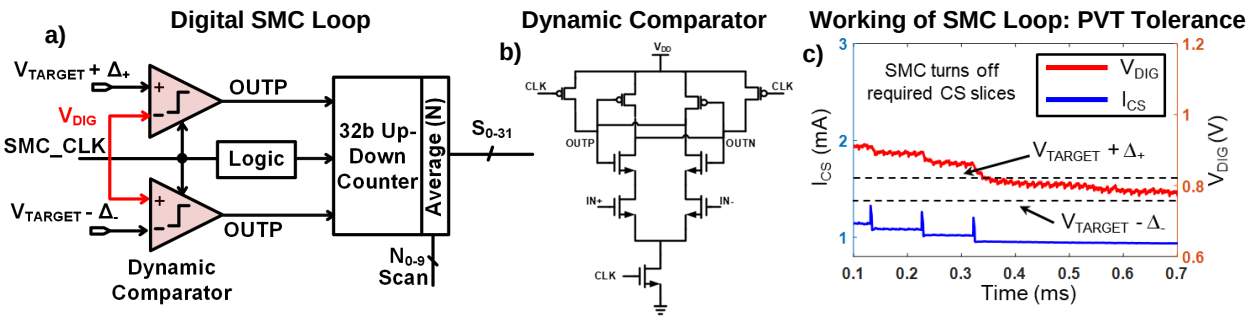


Figure 5.5. (a) Design of the Switched Mode Control Loop with guard bands, (b) Dynamic comparator checks if the V_{DIG} node goes out of the guard bands, (c) SMC logic turns on or off the required number of CS slices depending on the V_{DIG} voltage.

aids in low-frequency analog regulation without the need for a high-power shunt loop. The voltage at the V_{DIG} node is thus given as,

$$V_{DIG} = V_{BLEED} + V_{T_p} + \sqrt{\frac{2\Delta}{K_p(\frac{W}{L})_{BLEED}}} \tag{5.2}$$

where, V_{T_p} represent the threshold voltage of the PMOS bleed, and Δ being the excess current (quantization error) from the supply. Hence, with a large size of the bleed PMOS, the Eqn. 5.2 gets modified as,

$$V_{DIG} \approx V_{T_p} + V_{BLEED} \tag{5.3}$$

Now, the bleed should not be very large as it would unnecessarily drain extra current from the supply, increasing the power overhead without increasing the MTD. This is discussed in detail in Section III. G. The CS consists of 32 slices of PMOS and nominally 16 of them are turned on. The shunt path PMOS bias (near-threshold operation) as well as number of PMOS legs ON are scan controllable to analyze the effect of the extra bleed current on signature attenuation.

5.3.5 PVT Tolerance and SMC Loop

The design of the SMC loop is shown in Fig. 5.5(a). The slow digital SMC LDO tracks and regulates the voltage across the AES (V_{DIG} between $V_{TARGET}+\Delta_+$ and $V_{TARGET}-\Delta_-$) by turning ON or OFF the required number of PMOS CS slices. Two dynamic comparators (Fig. 5.5(b)) compare V_{DIG} with $V_{TARGET}+\Delta_+$ and $V_{TARGET}-\Delta_-$ respectively, and a 32-bit up-down counter with averaging (to control the loop frequency) controls the appropriate number of CS slices to be turned on. If $V_{DIG} > V_{TARGET}+\Delta_+$ for N SMC clock cycles, then a CS is turned ON. On the other hand, if $V_{DIG} < V_{TARGET}-\Delta_-$ for N SMC clock cycles, then a CS is turned OFF. Fig. 5.5(c) shows the working of the SMC loop where it turns OFF the required number of CS slices to reach the steady state (V_{DIG} within the guard band) after which it remains disengaged. The SMC loop can handle any process, voltage, and temperature (PVT) variations from chip-to-chip. At startup, CDSA requires $< 500\mu s$ to settle (Fig. 5.5(c)), which can be dummy operations. It should be noted that the SMC LDO is a low-BW loop (clocked at $< 10KHz$, V_{DIG} output pole at $\sim 106KHz$) and has a dead band of 50mV, such that it remains disengaged during the steady-state operation of the CDSA-AES circuit. The design of the dynamic comparators in the SMC loop which compares the V_{DIG} node voltage with the guard-band levels is shown in Fig. Fig. 5.5(c).

For the SMC loop, it needs to be noted that once the average current is set, that is, in steady state, the SMC is disengaged and the signature attenuation is given by the output resistance of the CS as well as the load capacitance.

5.3.6 Quantization vs. Key Leakage: Choice of CS Quantization

The average crypto current is a weak function of the secret key under attack and our goal is to ensure that any key-dependent variation is not reflected to the supply current. Hence, the quantization level is given as,

$$I_{CS_{N+1}} - I_{CS_N} > (\delta I_{AES_{avg}})_{max} \tag{5.4}$$

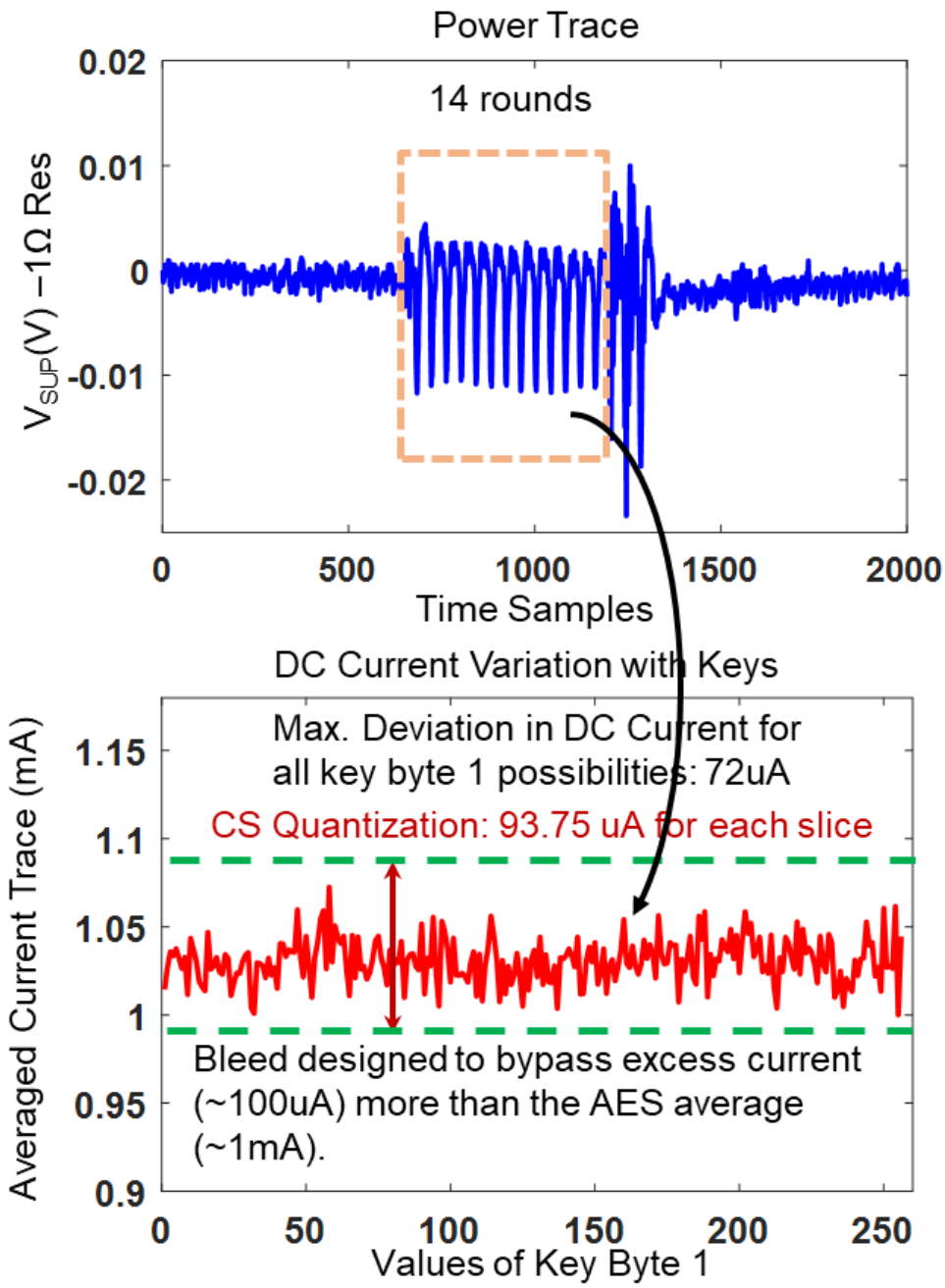


Figure 5.6. (a) Sample Power trace of the AES-256 showing 14 rounds of the encryption, (b) The average current of the trace during the 14 rounds is computed for all the 256 possibilities of the 1^{st} key byte. The CS quantization level (unit CS current) is designed to be higher than the maximum key-to-key variation in the average crypto current, so that any key-dependent information is not leaked through the power trace.

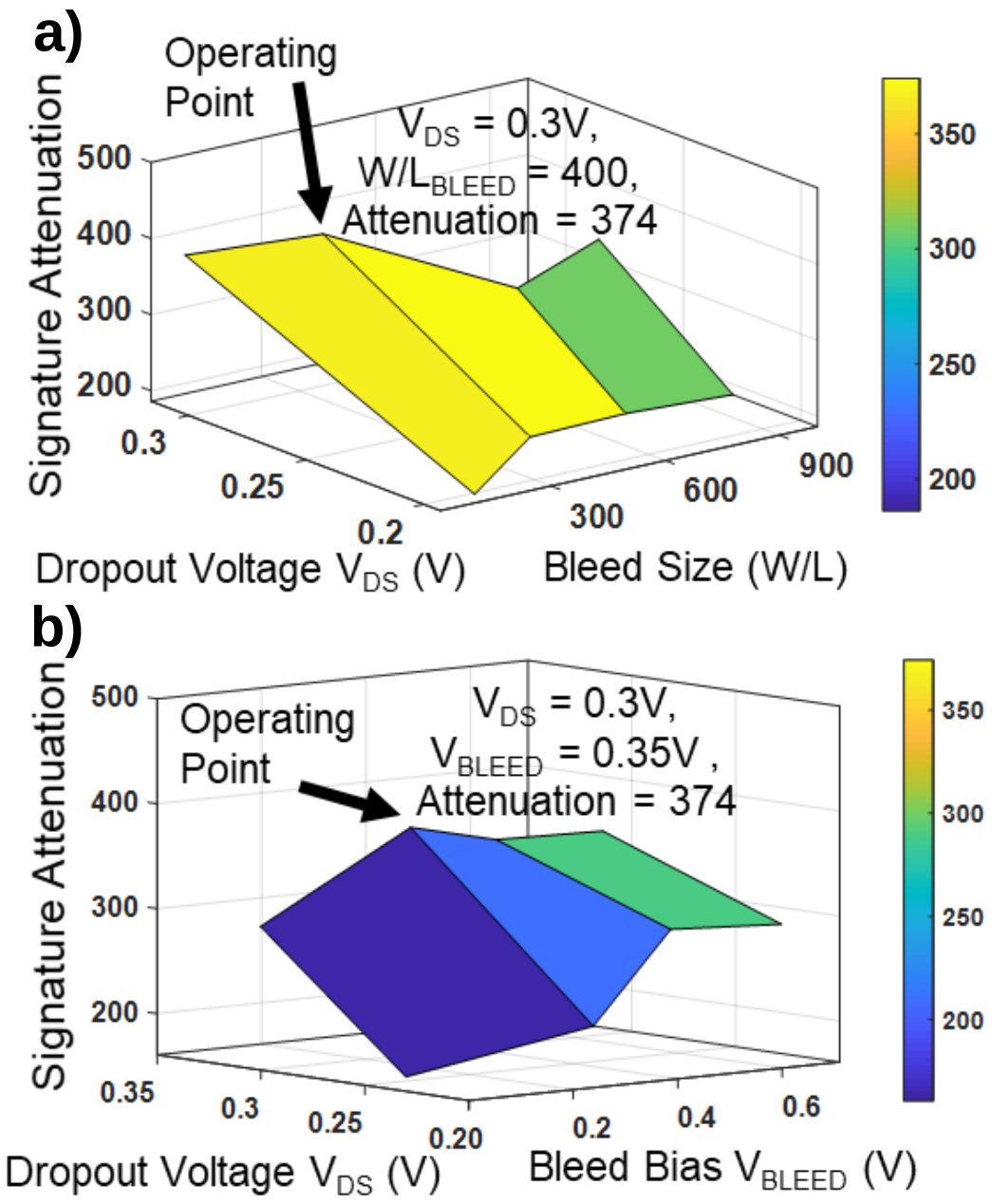


Figure 5.7. CDSA Design Space Exploration: (a) A dropout voltage (V_{DS}) of 0.3V across the current source and a bleed size of 400 is the most optimal choice, as a higher bleed size increases the current drawn from the supply and reduces the attenuation, (b) Bleed bias of 0.35 V is the most optimum beyond which it goes towards cut-off and the signature attenuation reduces.

where, $(\delta I_{AES_{avg}})_{max}$ is the maximum deviation in the average AES current for all the 256 different possibilities of a key byte. Thus, the unit current ($\sim 94\mu A$) of the CS is chosen such

that it is higher than the key-dependent variation in $I_{AES_{avg}}((\delta I_{AES_{avg}})_{max} \sim 72\mu A)$ (Fig. 5.6(a, b)), so that the key-dependent information in average DC current, is not transferred to supply current and is leaked by the bleed PMOS, making the design highly secure.

5.3.7 Design Space Exploration

Design space exploration of the CDSA-AES is shown in Fig. 5.7(a, b). As the bleed bias (V_{BLEED}) is increased from 0 to 200mV, the bleed current is reduced and the attenuation is increased as less current is drawn from the supply. Beyond 200mV, as the bleed PMOS goes towards cut-off, the attenuation reduces. Hence, the design space exploration reveals the optimum operating point at a dropout voltage (V_{DS}) of 0.3V across the CS stage and bleed bias (V_{BLEED}) of 0.35V.

5.4 White-Box EM Leakage Analysis & Local Signature Suppression

Most prior works on EM SCA attacks as well as countermeasures treat the crypto engine as a black box, without paying much attention to the cause of the EM leakage. However, a solid understanding of the genesis of the EM leakage from a crypto IC is necessary to develop an efficient low-overhead countermeasure.

5.4.1 Ground-Up Analysis

As we know, the acceleration of the electrons due to the switching of the output of the digital gates create create changing electric fields and magnetic fields, leading to EM radiation, according to the Maxwell's equations. Now, these generated EM fields depend on the metal layers inside the IC carrying the current, which act as dipole antennas and radiate. These switching currents passing through the metal layers undergo a transformation to create EM radiation and the magnitude of the fields depends on the dimensions of the metal layers. Higher-level metals are considerably thicker, and hence the EM leakage from these top metals has higher probability of detection using the commercially available EM probes (Fig. 5.8(b)). Fig. 5.8(a) shows the Intel 32nm metal-interconnect stack [97] as an example, where we see that as we move up the metal layers, the thickness increases and the top metal M_9 along with

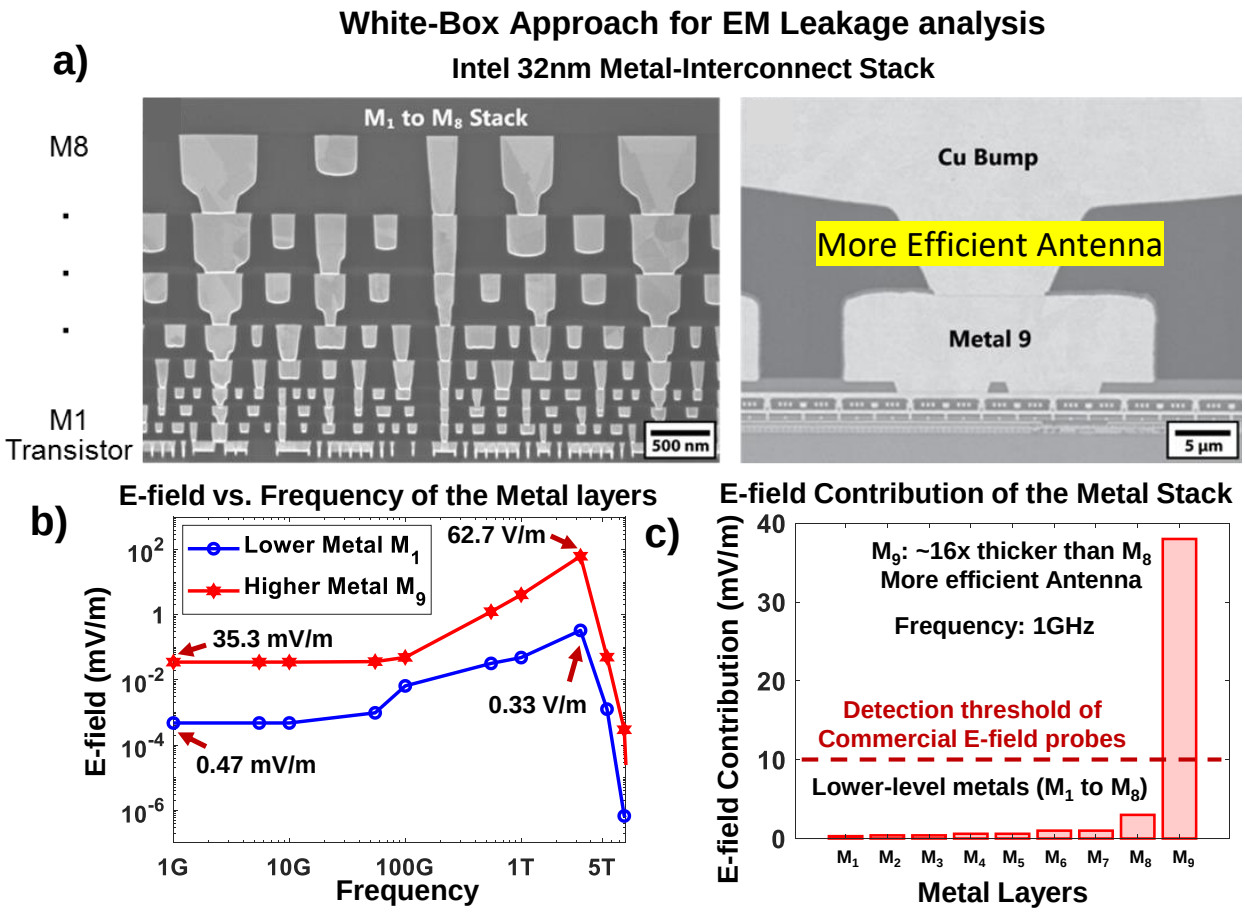


Figure 5.8. EM SCA White-box Analysis: (a) Intel 32nm metal-interconnect stack showing that the higher level metals are huge compared to the lower metal layers, (b) Higher metals are thicker and hence acts as a better antenna compared to the lower metals at the circuit-level operating frequency, (c) 3D FEM simulations using HFSS (1GHz, at a probe distance of $900\mu m$ from the chip) shows that the top level metals (M_9 and above for the Intel 32nm process) leak significantly more and the radiation can be detected using the commercially available EM probes.

the Cu bump is huge compared to the lower metals [37]. Using 3-D high frequency structure simulator (HFSS) to study the E-field contribution of the individual metal layers, it was observed that the contribution of the metal layers M_9 and above are detectable using the commercially available EM probes and hence these higher-level metal layers are vulnerable to EM side-channel leakages (Fig. 5.8(c)). The exact metal layer above which the fields are detectable will highly depend on the process as well as the sensing probe used. Moreover, the

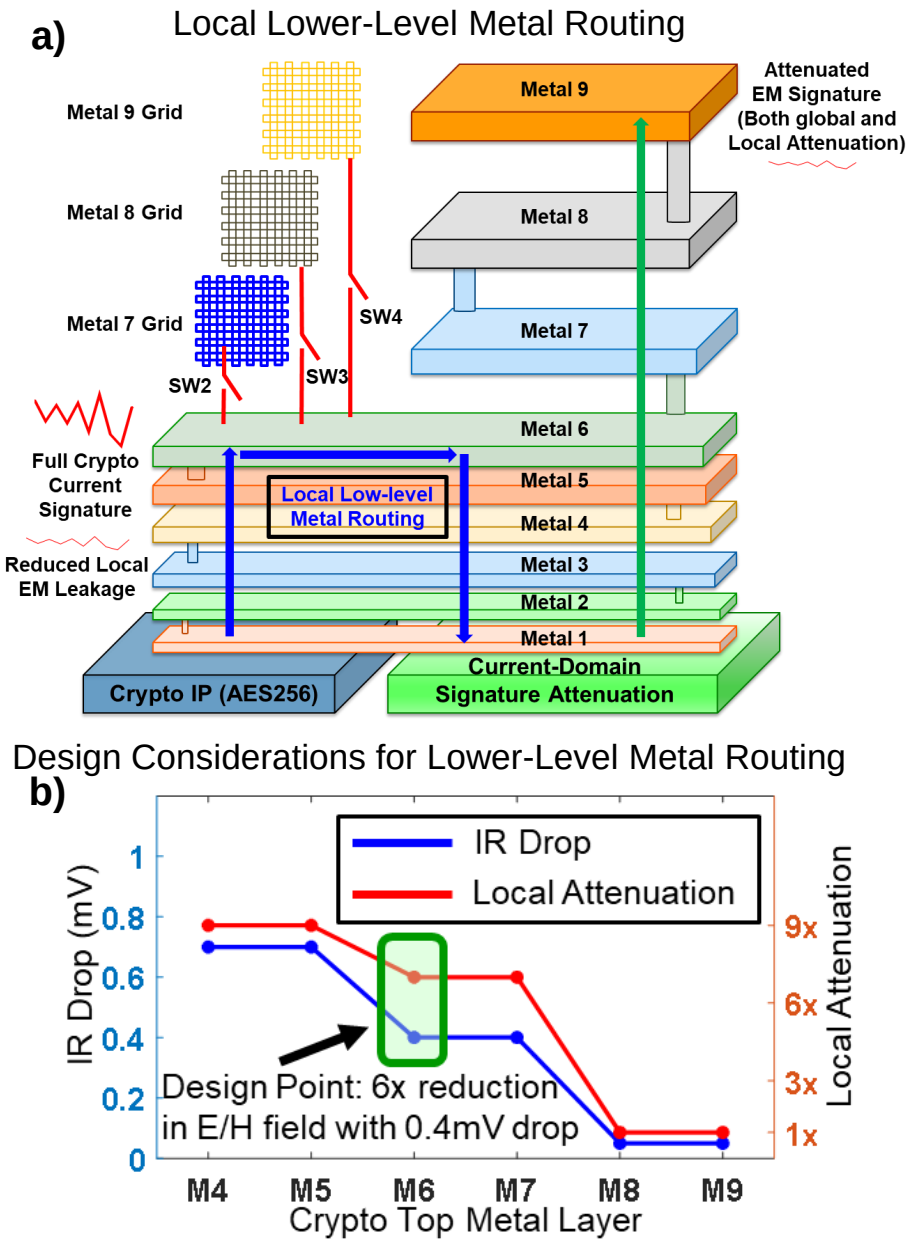


Figure 5.9. CDSA Design for Local EM Leakage Suppression: (a) The crypto core is routed within the lower-level metal layers and embedded within the locally routed CDSA which attenuates the crypto signature significantly before it passes through the higher level metal layers whose leakage can be detected by an external attacker. A mesh of metal layers 7, 8, and 9 are designed to evaluate the effect of higher-level metal layers on the EM radiation and SCA leakage. (b) Lower-level routing is performed up to metal M_6 considering the IR drop in the V_{DIG} node. The IR drop is shown considering a routing length of $100\mu m$.

Table 5.1. Modes of Operation of the Crypto Cores

Modes	Description	Configurability
Mode 1	Unprotected AES256	Separate Core
Mode 2	CDSA-AES256 with higher metal routing (only power protection)	SW2-4 ON (see Fig. 2)
Mode 3	CDSA-AES256 with local lower metal routing (both EM and power protection)	SW1 OFF, SW2-4 OFF (see Fig. 2)

ratio of electric/magnetic field strength reduction by routing through a lower metal layer, would also be heavily process technology dependent. However, the key take-away is that the top metal layers which are larger leak significantly more compared to the lower-level metal layers and hence should not be used to route unsuppressed correlated signature.

Through 3-D finite element method (FEM) simulation of metal traces using HFSS, it is validated that the EM leakage is a strong function of the metal dimensions carrying the correlated current [37]. As discussed in the previous section, the goal for EM SCA resilience is not to pass the correlated current through the higher-level metal layers. However, even if the sensitive signals are routed locally, power has to be routed to the external pins through higher metals. For only power SCA protection, we can utilize the current-domain signature attenuation (CDSA) hardware to suppress the correlated current signature, but if the routing is through the higher metals it would still radiate and would be vulnerable to EM SCA.

Equipped with this 'white-box' understanding of the genesis of the EM leakage and noting that the correlated current is the source of both power (at supply pin) and EM leakage (radiation through current path), this work embraces current-domain 'signature attenuation' (*CDSA*) with local lower-level metal routing as a low-overhead generic countermeasure against both EM and power side-channel attacks. Hence, we route the crypto engine within the lower-level metal layers and embed it locally within the CDSA hardware which suppresses the signature significantly before passing it through to the top-level metal layers.

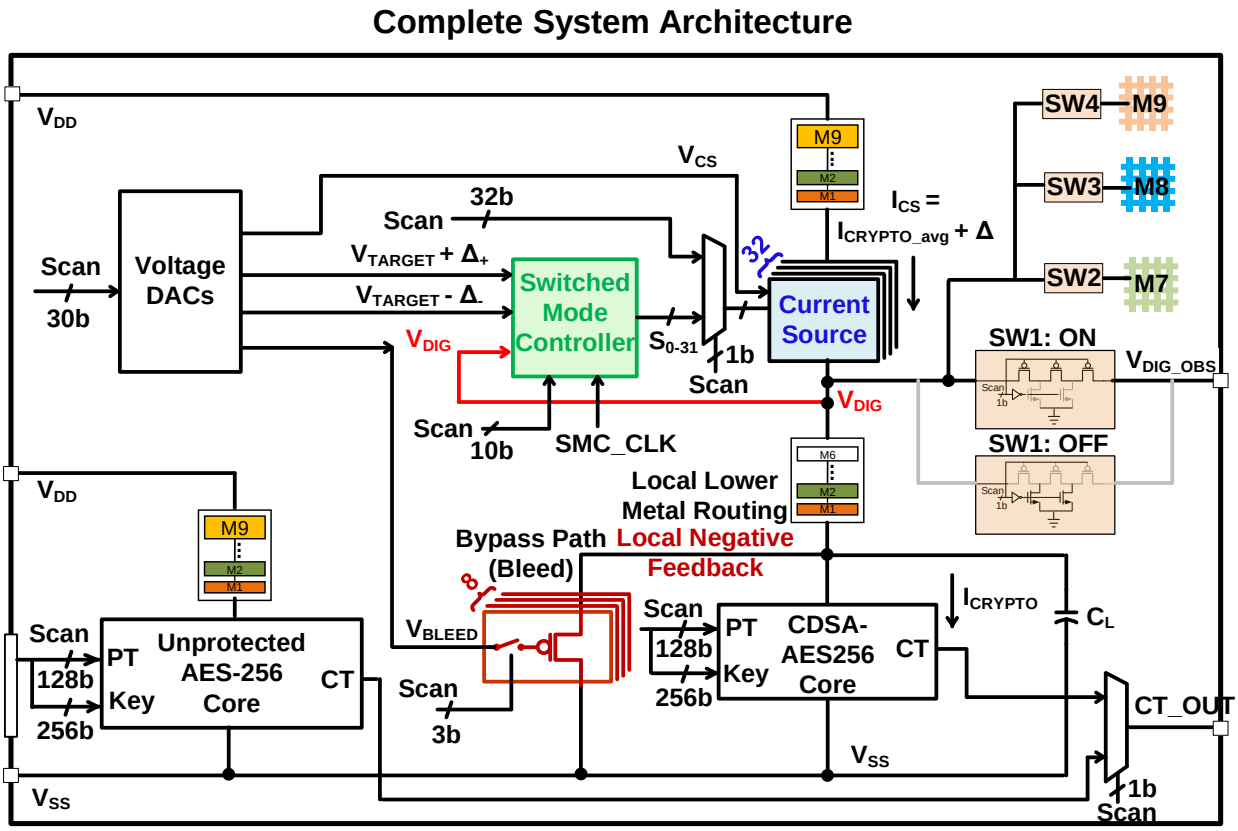


Figure 5.10. Complete System Architecture showing the unprotected AES-256 and the protected CDSA-AES256 cores. Highly isolating switch SW1 is designed to observe the V_{DIG} voltage across the AES-256. Other switches SW2-SW4 are designed to connect the AES core to the top metal mesh structures to evaluate the effect of higher metal layers on the EM SCA leakage.

5.4.2 CDSA Design for EM SCA Protection: Local Lower-Level Metal Routing

The previous technique of active inline current domain signature suppression protects against power and the global EM leakage. Here, we will look into the design strategy to prevent against local EM leakage.

As seen from Fig. 5.9(a), the crypto IP (AES-256 for this work) is routed within the lower-level metal layers (M_1 to M_6) and then the correlated current is passed through the physically-close CDSA block which is also routed locally within the lower metals. The arrows in the figure indicate the direction of flow of the current. The correlated local EM leakage is significantly suppressed by the CDSA within the lower metal layers (up to M_6), and it is

then passed through the higher-level metal layers to connect to the pin. A mesh of metals 7, 8 and 9 is designed on top of the crypto core to evaluate the contribution of the top metal layers to EM radiation.

Lower metal routing (up to M_6) provides a local attenuation of $\sim 7\times$ (compared to passing the signature directly to M_9 which has larger dimensions and radiates more). The local routing of the CDSA with lower-level metal layers has trade-offs with the IR-drop, as shown in Fig. 5.9(b). Routing the V_{DIG} node with M_6 ensures that the additional IR-drop is limited to $< 0.4mV$. The load capacitor (C_L) uses only MOS cap (lower metal layers) rather than MIM (top metal layers) so that the EM radiation is minimized. This comes at the expense of some extra area and leakage power of the MOS cap (compared to MIM cap) which is a fundamental trade-off to ensure high EM SCA protection. For EM SCA, MIM capacitors should never be used on correlated current node, as the MIM capacitor plate with the correlated sensitive signature, effectively turns into a radiating element, leaking critical correlated information.

5.5 System Architecture

The full system architecture is shown in Fig. 5.10(a). It consists of both unprotected and protected AES-256 implementations. The architecture of the parallel AES-256 is shown in Fig. 5.11(a). AES-256 is implemented with parallel data-paths to provide high performance and requires 14 cycles per encryption. The top-level interface for external programmability and observability is shown in Fig. 5.11(b). To verify the correct working of the AES-256, we have an output ciphertext (CT Serial Out) mode, where the ciphertext is streamed out serially, as shown in Fig. 5.14.

As seen from Fig. 5.10(a), the CDSA-AES has scan-controlled highly isolating switches (SW1) to connect the V_{DIG} node to an external pin for observability (SW1 ON) or disconnect without leaking EM during normal operations (SW1 OFF). Similar highly isolating switches (SW2-4) are kept on top of the crypto core for the protected implementation to analyze the effect of higher level metals on the EM leakage.

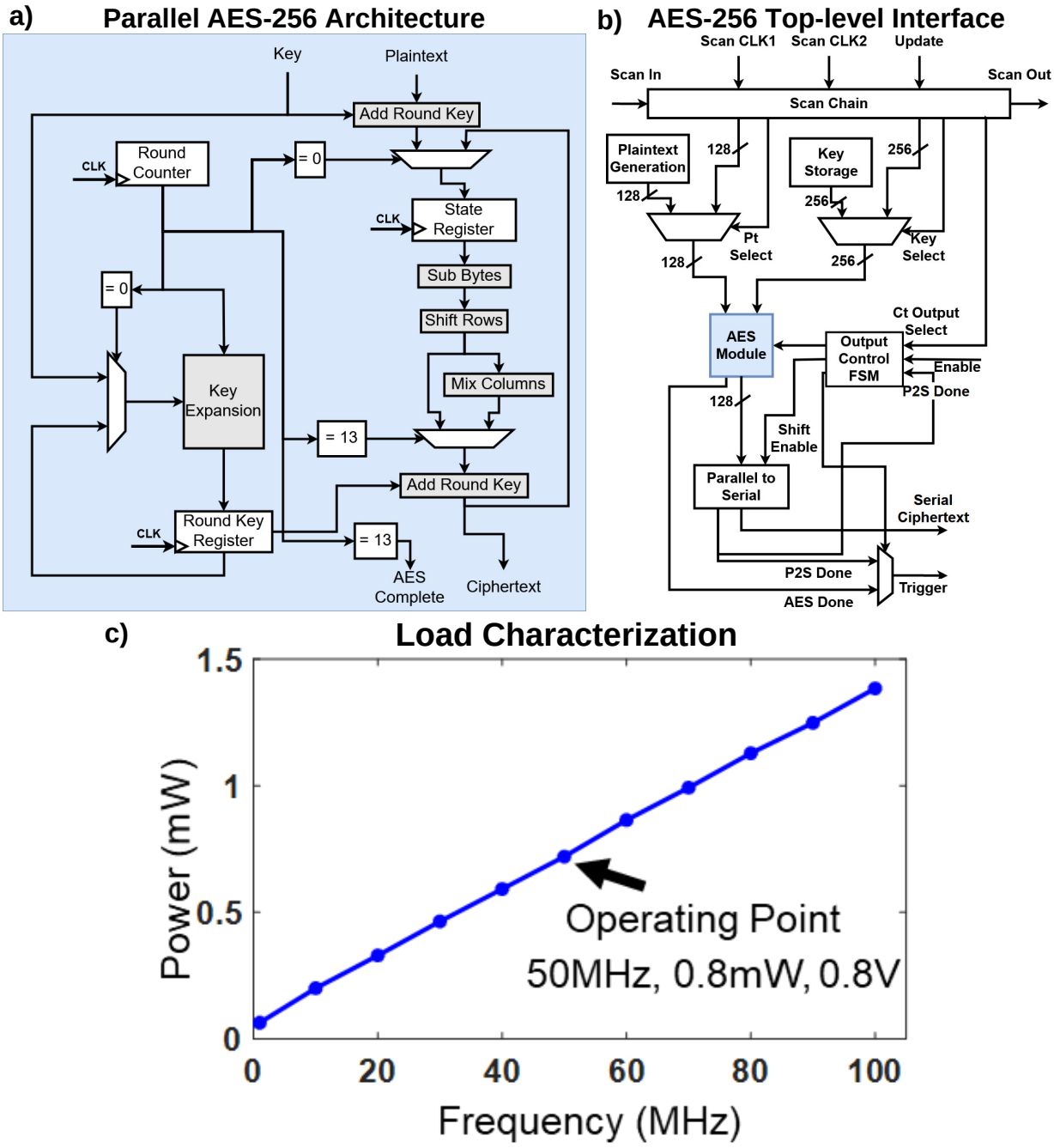
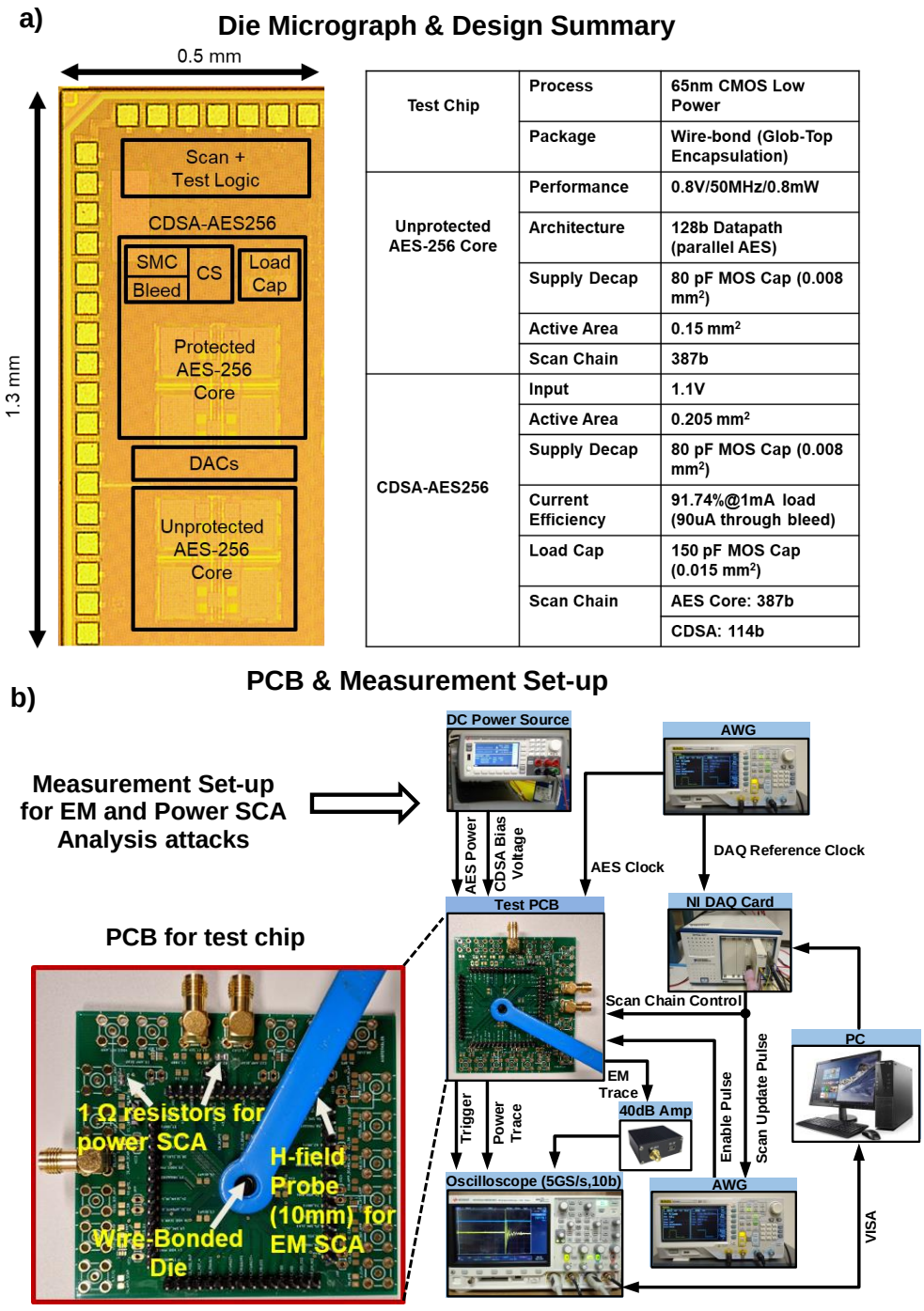


Figure 5.11. (a) Parallel AES-256 Architecture, & (b) Top-level Interface. (c) The AES-256 is powered at 0.8V at 50MHz and consumes 0.8mW power.

The system has three modes of operation as shown in Table 5.1. In mode 1, the unprotected AES-256 is operated. Mode 2 is the CDSA-AES with higher-level metal routing



Test Chip	Process	65nm CMOS Low Power
	Package	Wire-bond (Glob-Top Encapsulation)
Unprotected AES-256 Core	Performance	0.8V/50MHz/0.8mW
	Architecture	128b Datapath (parallel AES)
	Supply Decap	80 pF MOS Cap (0.008 mm^2)
	Active Area	0.15 mm^2
	Scan Chain	387b
CDSA-AES256	Input	1.1V
	Active Area	0.205 mm^2
	Supply Decap	80 pF MOS Cap (0.008 mm^2)
	Current Efficiency	91.74%@1mA load (90uA through bleed)
	Load Cap	150 pF MOS Cap (0.015 mm^2)
	Scan Chain	AES Core: 387b
		CDSA: 114b

Figure 5.12. (a) Die micrograph of the system in 65nm CMOS process and design summary, (b) PCB and the measurement set-up for EM and power SCA attacks.

(power protected), and mode 3 (default operation mode) is the fully protected implementation with lower metal routing and provides both EM and power SCA protection.

5.6 Measurement Results: Efficacy of the Countermeasure

The die micrograph of the test chip fabricated in TSMC 65nm technology is shown in Fig. 5.12(a). The package was wire-bonded on the PCB with glob-top encapsulation and consumes an active area of $0.15mm^2$.

The PCB and measurement set-up is shown in Fig. 5.12(b). For power SCA attacks, we mount 1Ω resistors at the power supply of both the unprotected and protected AES-256. A H-field probe of 10mm loop diameter is used to measure the EM leakage from the IC while performing encryption. For our EM measurements, we had compared with Tekbox probes of 5mm, 10mm, and 20mm [100], and the 10mm probe was the most optimal choice as it picked the most EM signal. The measurement set-up consists of an oscilloscope for capturing the traces, and is connected through an external 40dB wideband amplifier for the EM trace capture.

The unprotected AES is powered with 0.8V input and consumes $\sim 1mA$ average current at 50MHz, as shown in Fig. 5.11(c).

5.6.1 Time-Domain Measurement Results

Fig. 5.13 shows the time-domain measurement results for both the unprotected and protected AES-256. The power trace for the unprotected AES clearly shows the 14 rounds of the encryption, which is $\sim 150mV$ in amplitude, while the CDSA-AES power signature is attenuated by $> 350\times$ and remains below the noise floor of the oscilloscope. Observing the V_{DIG} across the AES engine, we can see the 14 rounds of the AES, however, we choose to tolerate these fluctuations at V_{DIG} with a smaller C_L to reduce area overhead, and instead have the high impedance (r_{ds}) CS on top, which ensures that the correlated signatures are not reflected to the supply current, as seen from Fig. 5.13. Also, for the EM signature, the 14 rounds are clearly visible for the unprotected implementation, while it remains below the noise floor for the CDSA-AES.

Both the unprotected and protected AES-256 can be operated in the Ciphertext (CT) Serial Out Mode, as shown in Fig. 5.14. In this mode, the 128-bit CT is serially output after the 14 cycles of the each encryption.

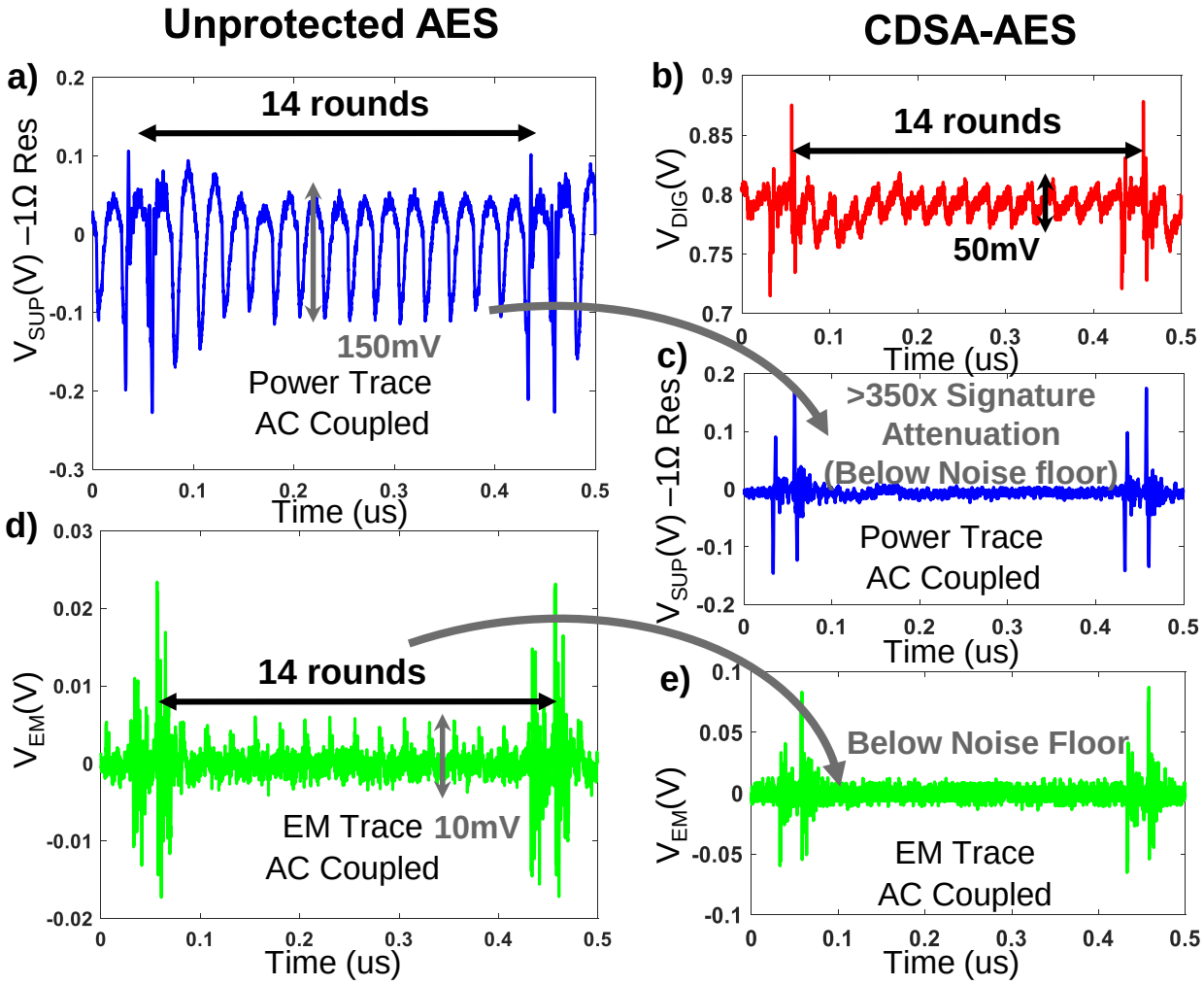


Figure 5.13. Time-Domain Measurement Results: (a-c) Power trace from the unprotected AES-256 clearly shows the 14 rounds of the encryption (a), and the power trace has an amplitude of 150mV, which is significantly attenuated by a factor of $> 350\times$ and the power trace for the CDSA-AES256 remains below the noise floor as shown in (c). The intermediate node V_{DIG} still shows the 14 encryption rounds (b), however it is only for observability and is inaccessible to an attacker. The high output impedance of the CS stage on top ensures that the fluctuation at the V_{DIG} is highly suppressed at the supply pin available to an attacker. (d, e) The unprotected EM trace clearly shows the 14 rounds of the AES-256 (d), however for the CDSA-AES256 (e), the EM trace is below the noise floor.

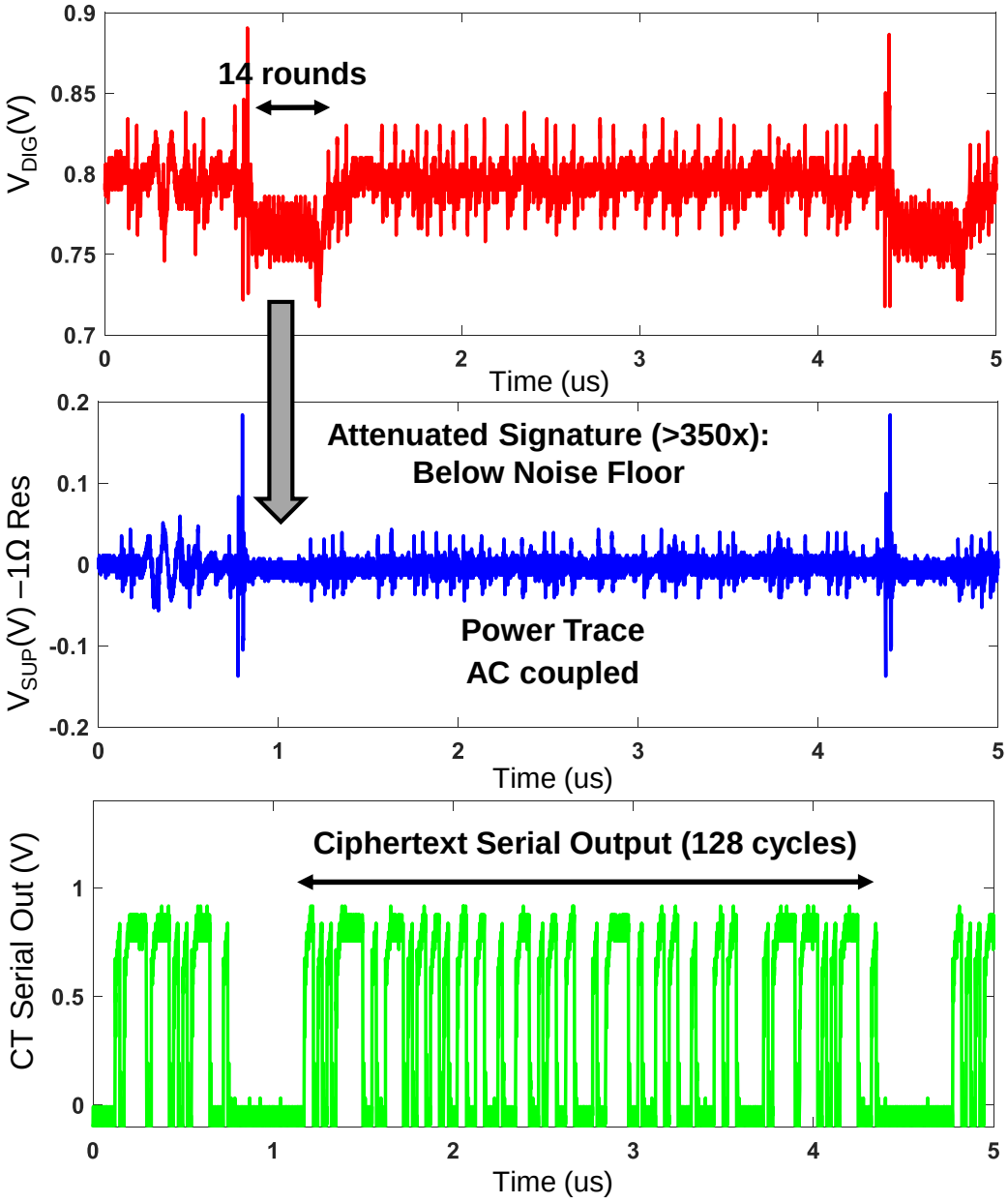


Figure 5.14. The AES-256 can operate in a ciphertext serial output mode (CT Serial Out), where it outputs the 128-bit ciphertext in 128 cycles after the 14 rounds of the encryption.

5.6.2 EM & Power Side-Channel Analysis and Attacks

Now, let us look into the SCA resiliency of the unprotected and protected implementations. Both time and frequency-domain CPA and CEMA are performed. Test Vector Leakage assessment is also shown for both the unprotected and protected implementations.

Attack Model

For both CPA/CEMA attacks, we use the HD model of the last 2 rounds (HD between the CT and the output of the 13^{th} round) of the AES-256. For the frequency-domain attack, the traces are passed through a narrowband filter of 10MHz bandwidth with the center frequency sweeping from 10MHz to 1GHz (Fig. 5.15).

CPA Attacks & Power-TVLA

Fig. 5.15 shows the hamming distance (HD) attack model used between the last 2 rounds of AES (13th round output and the ciphertext) and a correlational power attack (CPA) on the unprotected AES implementation shows an MTD of 8K, while the CDSA-AES cannot be broken even after 1B traces (without any intentional noise injection). While all key bytes show similar trends, we demonstrate the efficacy of the countermeasure with attacks on the 1st key byte. Fixed vs. random Test Vector Leakage Assessment (TVLA) on the unprotected AES shows a t-value of 1056 after 200M traces compared to ~ 12 for CDSA-AES. Frequency-domain CPA with windowed FFT has been performed with a window size of 10MHz and the center frequency is swept from 10MHz to 1GHz. However, the correct key byte was not revealed for any frequency band, even after 1B traces, showing an MTD improvement of $\sim 125,000\times$.

CEMA Attacks & EM-TVLA

CEMA on the unprotected AES shows an MTD of $\sim 12K$, while the CDSA-AES is not broken after 1B measurements (Fig. 5.15). The results were also verified with frequency-domain CEMA. TVLA on the unprotected AES shows a t-value of 961 compared to a t-value of 6 for the CDSA-AES (with lower metal routing – Mode 3: Fig. 5.10(b)). The effect of higher metal layer routing on EM leakage is analyzed by turning on highly-isolating switches (SW2-SW4) that connects V_{DIG} to higher metal radiating structures (Fig 2). In this Mode (2) with all M7-M9 connected, the EM leakage crosses the threshold of 4.5 within 20M traces, compared to $\sim 170M$ traces for mode 3, demonstrating the effect of local attenuation

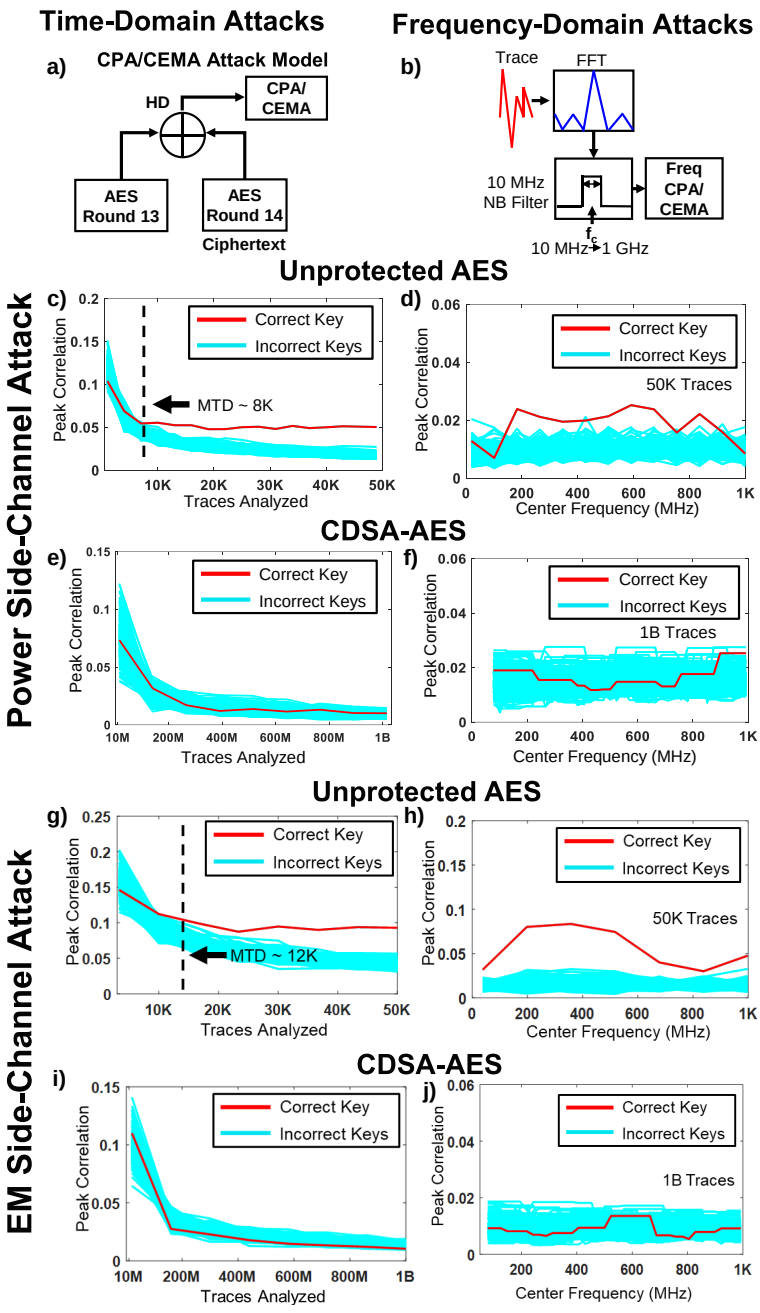


Figure 5.15. EM & Power SCA Attack Evaluation: (a) Attack model for CPA/CEMA. (b) Frequency domain CPA/CEMA. (c) Time-domain CPA, (d) frequency domain CPA on unprotected AES. (e) Time-domain CPA and (f) frequency domain CPA on the protected AES. (g) Time-domain CEMA on the unprotected and (h) the protected CDSA-AES. (h) Frequency-domain CEMA on the unprotected AES, (j) the protected implementation remains secure even after $1B$ traces.

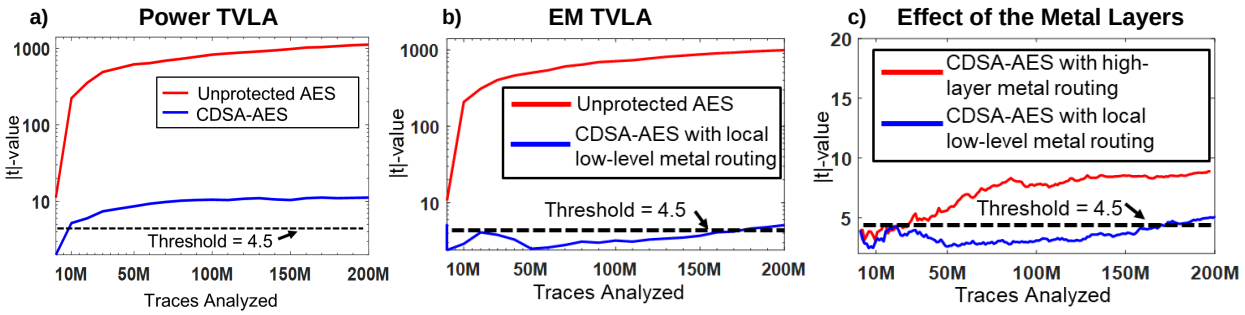


Figure 5.16. Power & EM fixed vs. random Test Vector Leakage Assessment (TVLA): (a) The unprotected AES-256 has a t-value of > 1000 with $200M$ analyzed power traces, while it remains ~ 10 for the CDSA-AES256. (b) EM TVLA on the unprotected AES-256 shows a t-value of > 1000, while the t-value protected implementation (Mode 3, with lower metal routing) remains ~ 5 for $200M$ analyzed traces. (c) CDSA-AES with higher-level metal routing shows $> 7\times$ higher leakage compared to the lower-level routing, as it crosses the t-value threshold of 4.5 within $20M$ traces in mode 2 while the fully protected implementation (mode 3) crosses the threshold in $170M$ traces.

($> 7\times$) and the significance of the local lower metal routing for EM SCA protection (Fig. 5.15).

5.6.3 Comparison with State-of-the-Art

Compared to the existing state-of-the-art circuit-level countermeasures, current domain signature attenuation (CDSA) with lower-level metal routing provides $100\times$ higher MTD (Fig. 5.17) with comparable power and area overheads (Table5.2). CDSA-AES has been evaluated against both time-domain and frequency-domain attacks for power as well as EM SCA. This is also a generic countermeasure and can be extended to any other crypto engines without any performance degradation.

It should be noted that this IC is designed in 65nm process, while some of the previous works were performed in 130nm CMOS technology. At lower technologies, the supply voltage (V_{DD}) is lower and the output resistance (r_{ds}) of a transistor gets reduced. To achieve the same r_{ds}, the size of the current source (CS) has to be enhanced, leading to an increase in the area overheads for 65nm compared to the 130nm. Also, since the VDD is lower, for iso-dropout voltage (V_{DS}), the power overhead would be increased at 65nm compared to the

Table 5.2. Comparison with State-of-the-Art

Parameter			This Work	JSSC'20 [120]	JSSC'18 [125]	JSSC '10 [106]	VLSI'15 [124]
Countermeasure Technique			Current Domain Signature Attenuation	Digital LDO with randomization	Integrated Buck Regulator	Switched Capacitor Current Equalizer	Charge Recovery Logic
Process			65nm CMOS	130nm CMOS	130nm CMOS	130nm CMOS	65nm CMOS
Crypto Algorithm			AES-256	AES-128	AES-128	AES-128	AES-128
Standalone AES Power/Frequency			0.8mW @ 50MHz, 0.8V	10.9mW @ 80MHz, 0.84V	10.5mW @ 40MHz	33mW @ 100MHz	138mW@1.32 GHz
Design Overheads	Area		36.7%[c]	36.9%[b]	1%[a]	33%	25%
	Capacitor		150pF MOS	1.9nF MIM	3.2nF MIM	300pF	-
	Power		49.8%[c]	32%	5%*[a]	20%	30%
	Perf.		0%	10.4%	3.33%	50%	0%
SCA Analysis	Time/Freq Domain		Time, Freq	Time, Freq	Time, Freq	Time	Time
	MTD	Power	**>1B (>125,000x)**	8M (4210x)	>100K (20x)	>10M (2500x)	940K (251x)
		EM	**>1B (>83,333x)**	6.8M (136x)	-	-	-
	Attack Mode		Power/EM	Power/EM	Power	Power	Power

[a]Does not include regulator area/power, [b]Does not include MIM Cap area, [c]Power overhead includes the dropout voltage across CS, the excess bleed current drawn during the steady-state operation, as well as the V_{DIG} guard-banding to ensure no performance degradation. Area overhead includes the load cap area, CS, SMC loop, and the bleed path.

130nm. In addition, the average load current of the crypto core ($I_{CRYPTO_{avg}}$) is also reduced, and hence the power overhead would be worse at 65nm. Overall, the design trade-offs at 65nm node are worse compared to the 130nm CMOS process. Hence, as we scale down technologies, we need more scalable circuits, and hence digital-friendly implementation of the CDSA should be developed, which is part of the future work.

5.7 Conclusion

The proposed countermeasure provides both power and EM SCA immunity utilizing in-line active signature suppression and local lower-level metal routing leading to a 100× MTD improvement over the state-of-the-art (Fig. 5.17). CDSA-AES256 acheives $> 1B$ MTD against CPA and CEMA attacks, which is an improvement of $> 125,000\times$ and $83,333\times$ respectively compared to the unprotected implementation. It is a low-overhead countermeasure and incurs a power overhead of 49% and an area overhead of 36%. The power overhead is mainly due to the dropout voltage across the current source, and the area overhead is due

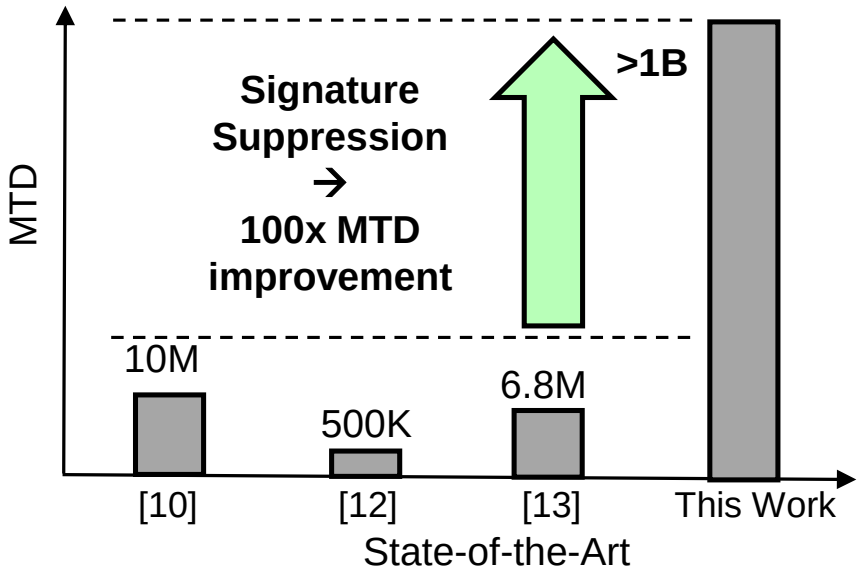


Figure 5.17. Summary: Improvement over the State-of-the-Art

to the restriction that we use only MOS capacitors instead of MIM which are implemented in the higher metal layers and can leak critical information. Finally, the presented CDSA hardware is a generic countermeasure and can be extended to any crypto algorithm as a wrapper around it (useful for legacy protection), without any performance penalty.

In the next chapter, we will analyze the security of CDSA-AES256 against advanced ML SCA attacks.

6. DEEP LEARNING SIDE-CHANNEL ATTACK EVALUATION ON CURRENT DOMAIN SIGNATURE ATTENUATION HARDWARE BASED AES-256

Most of the materials in this chapter have been extracted verbatim from the paper:
1. Debayan Das, Anupam Golder, Josef Danial, Santosh Ghosh, Arijit Raychowdhury, Shreyas Sen, Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS, *IEEE Custom Integrated Circuits Conference (CICC)*, 2020.

This chapter, for the first time, demonstrates an efficient circuit-level countermeasure to prevent deep-learning based side-channel attacks (DLSCA) on encryption devices. Machine learning SCA, particularly DLSCA attacks have been shown to be extremely effective as it can potentially reveal the secret key of the cryptographic device with a single trace. This work presents a current-domain signature attenuation (CDSA) hardware embedding an AES256 engine fabricated in 65nm CMOS technology to suppress the current signature by $> 350\times$ before it reaches the power supply pin accessible to an attacker. Measurement results shows that a 256-class deep neural network (DNN) model for DLSCA attack can be fully trained ($> 99.9\%$ test accuracy) using only $< 5K$ power traces from the unprotected AES256, while the DNN model for the protected CDSA-AES256 could not be trained even with 10M traces.

6.1 Background

6.1.1 Motivation

DLSCA utilizes a DNN model for each key byte (for AES256) by training it on traces collected by varying the key byte [64]. As shown in Fig. 6.1(a), power traces for profiling (training) the 256-class DNN are captured from the test chip running AES256 (protected/unprotected mode) with a fixed plaintext and varying the 1st key byte and labeling each trace with the corresponding key byte value. During the DLSCA attack phase, unseen traces are fed to the trained DNN to predict the correct key byte. Fig. 6.1(b, c) shows an overview of

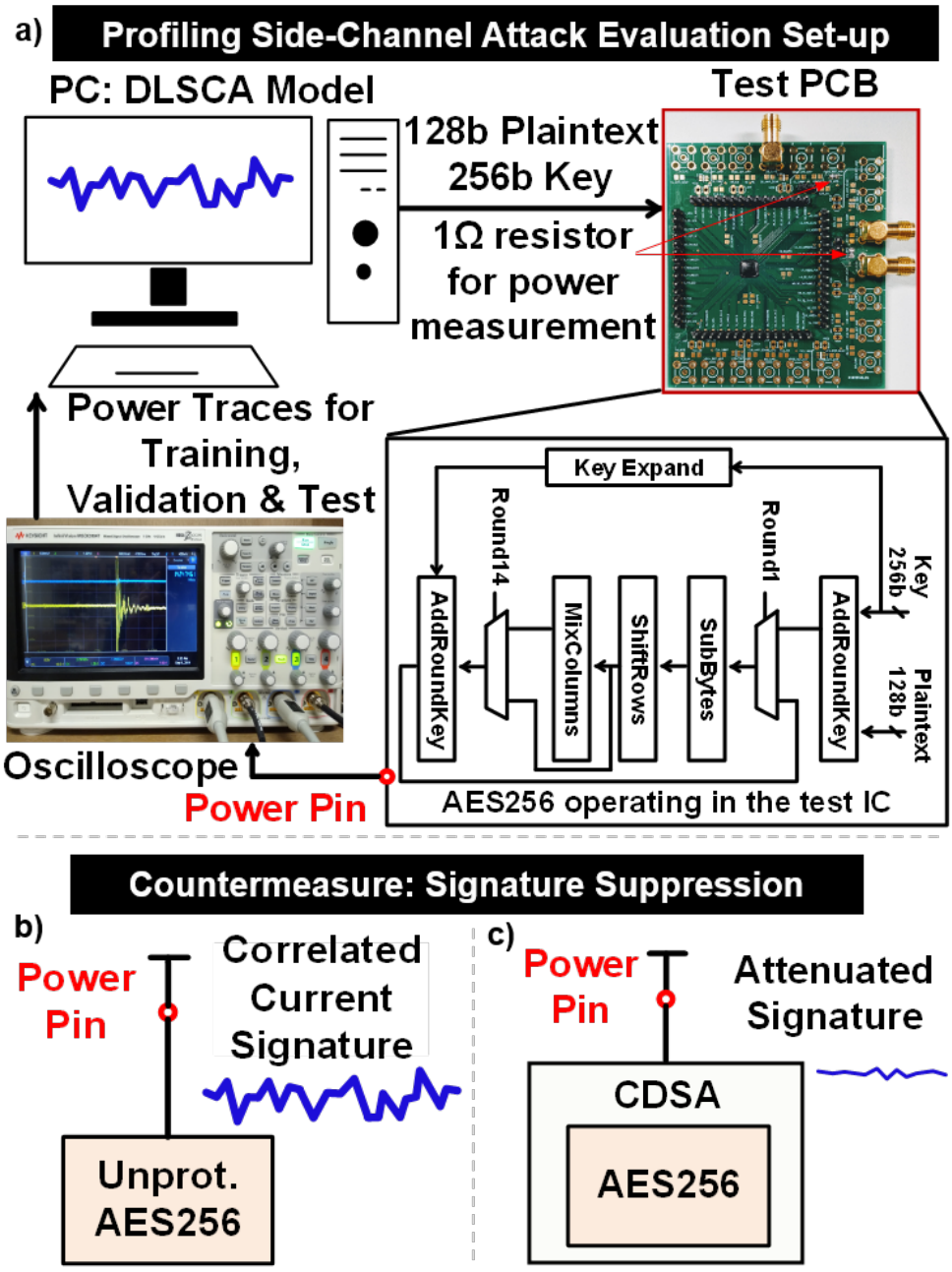


Figure 6.1. (a) Deep-Learning based SCA attack set-up on the AES256 with the 65nm test chip. (b, c) Overview of the CDSA hardware.

the proposed CDSA circuit, which attenuates the correlated current signature significantly, motivated by the fact that the minimum traces to disclosure (MTD) is inversely proportional to the square of the signal to noise ratio (SNR): $MTD \propto \frac{1}{SNR^2}$ [42].

6.1.2 Contribution

The key contributions of this work are:

- This work utilizes CDSA hardware involving a high output impedance current source (CS) on top of a crypto engine to provide $> 350\times$ signature attenuation in 65nm CMOS.
- DLSCA attack is demonstrated on an unprotected AES256 engine in 65nm CMOS using only $< 5K$ measured power traces to train the 256-class DNN.
- Measured results from the CDSA-AES demonstrate high DLSCA resilience as the DNN could not be trained even with $10M$ traces. Moreover, it is a generic low area/power overhead SCA countermeasure and can be extended to other crypto algorithms without any performance degradation.

6.2 Background & Related Work

Existing logical and architectural countermeasures involving time-domain or clock-jitter based obfuscations have been shown to be defeated using convolutional neural networks (CNNs) which learns the side-channel leakage even in presence of trace misalignments [67]. Also, masking-based countermeasures have been shown to be broken using DNNs [68], [69]. Circuit-level on-chip power SCA countermeasures include charge recovery logic [124], switched capacitor current equalizer [133], [106], integrated voltage regulator (IVR) [108], and all-digital low-dropout (LDO) regulator [134], which suffer from performance degradation, high power/area overheads because of large embedded passives, as well as EM leakage from large metal-insulator-metal (MIM) capacitor top plates. Simulations of shunt LDO based regulators have been shown to be effective for power SCA resistance [42]. None of these have been evaluated against DLSCA attacks.

Recently, CDSA has been shown to be extremely resilient shown against traditional non-profiled CPA/CEMA attacks with MTD $> 1B$ traces [40]. This work, for the first time, evaluates the efficacy of the CDSA hardware against DLSCA attacks on AES256.

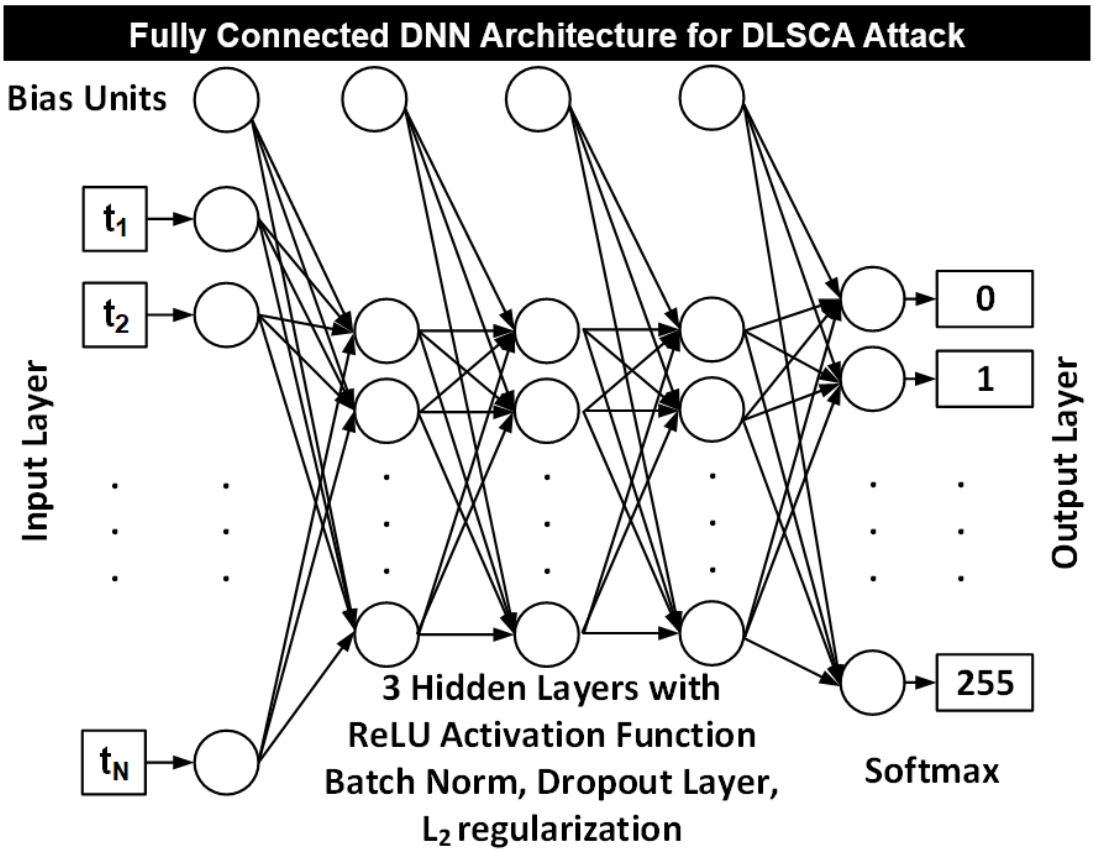


Figure 6.2. DNN Architecture for the DLSCA attack on the unprotected AES256 and CDSA-AES256.

6.3 DLSCA Attack on the Unprotected AES256

The 65nm test chip contains both unprotected and protected (CDSA) implementations of AES256 (refer Fig. **??**(a)). For profiling, we capture power traces from the unprotected core and build the DNN model. Once the training is completed, the DNN model can then be used to attack (classify unseen traces).

6.3.1 DNN Architecture

Fig. 6.2 shows the DNN architecture for the DLSCA attack. The input layer consists of 250 neurons (number of time samples in each measured power trace), followed by three hidden layers, each with Rectified Linear Unit (ReLU) non-linear activation, batch normalization,

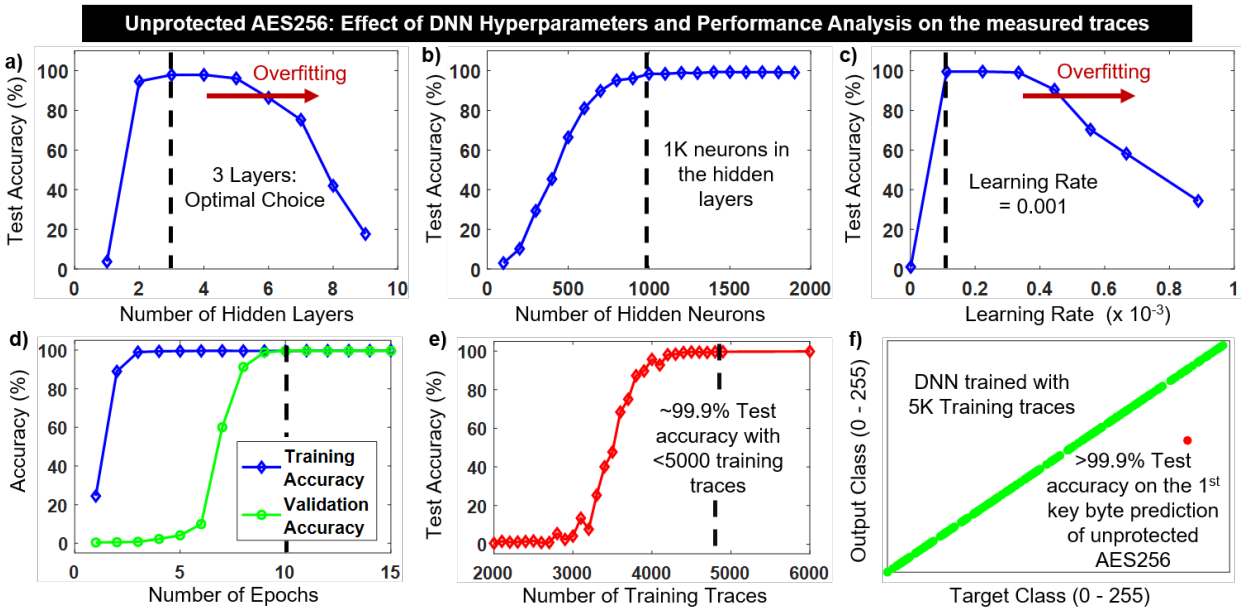


Figure 6.3. DLSCA attack on the unprotected AES256: (a-c) Effect of the hyperparameters (number of hidden layers, hidden neurons in each layer, learning rate) on the test accuracy of the fully-connected DNN for 5K training traces. (d) Training/Validation accuracy reaches 99.9% within 10 epochs with 5K training traces. (e) Test accuracy of the DNN reaches $\sim 99.9\%$ with $< 5K$ training traces with 10 epochs. (f) Confusion plot of the test traces showing $> 99.9\%$ test accuracy of the DLSCA.

a dropout layer (20%), and L_2 regularization to prevent overfitting and finally the output layer with 256 neurons, which predicts the correct key byte in a single trace utilizing the softmax function.

6.3.2 Choice of Hyper-parameters

Fig. 6.3(a-c) shows the effect of the hyperparameters on the DNN test set accuracy. Three hidden layers with $1K$ neurons each and a learning rate of 0.001 is the most optimal choice for the unprotected AES256 traces.

6.3.3 Performance Analysis

Fig. 6.3(d, e) shows that the training and validation accuracy of the DNN reaches $> 99.9\%$ within 10 epochs, and the test accuracy on the unseen traces reaches $\sim 99.9\%$,

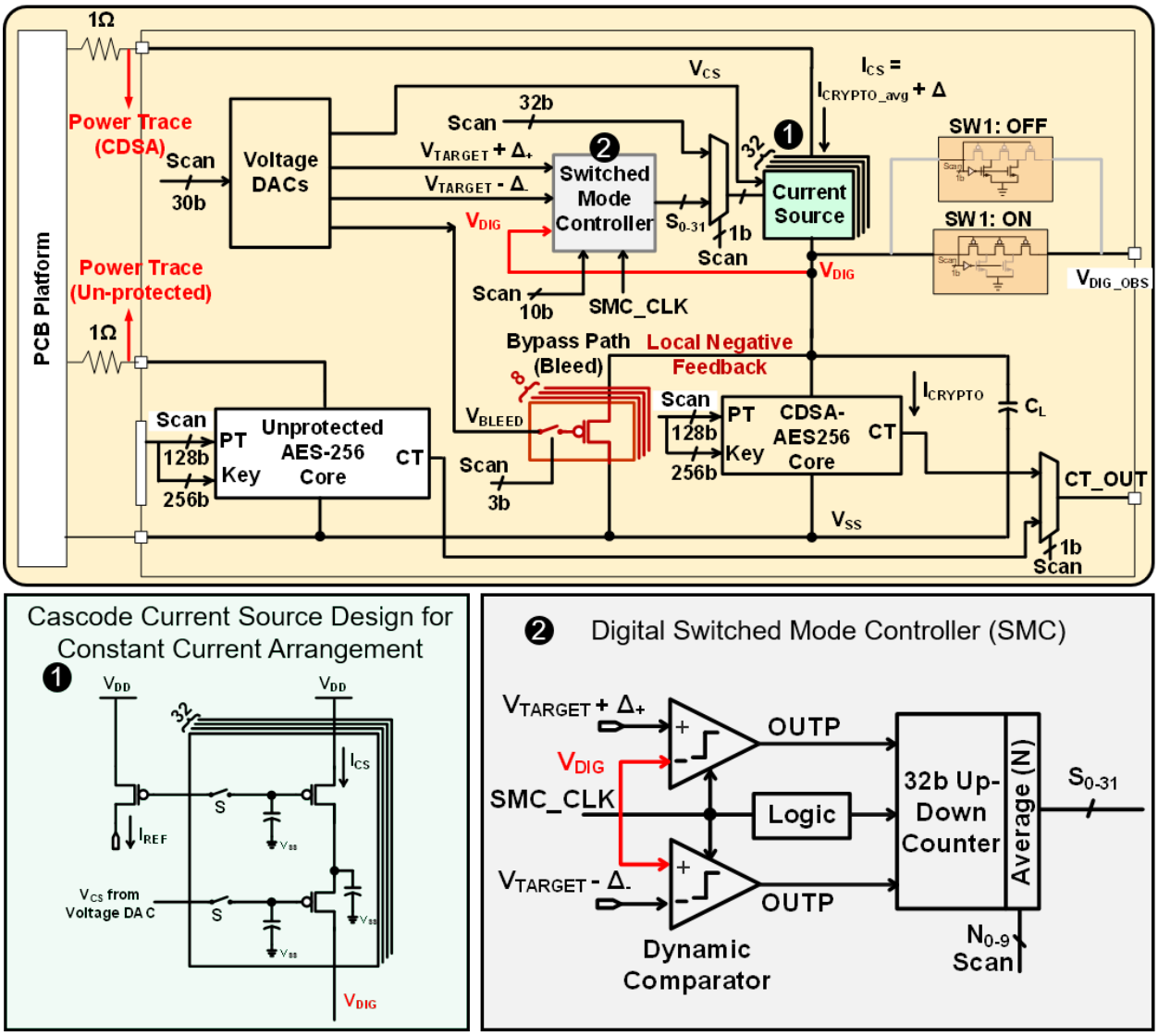


Figure 6.4. System architecture showing the circuit details of the cascode current source (CS) and the digital switched mode control (SMC) loop.

with only $< 5K$ training traces. The test confusion plot (Fig. 6.3(f)) reveals that only 1 key byte value (marked in red) out of the 256 was misclassified by the DNN, demonstrating a successful DLSCA attack on the 1st key byte of the unprotected AES256.

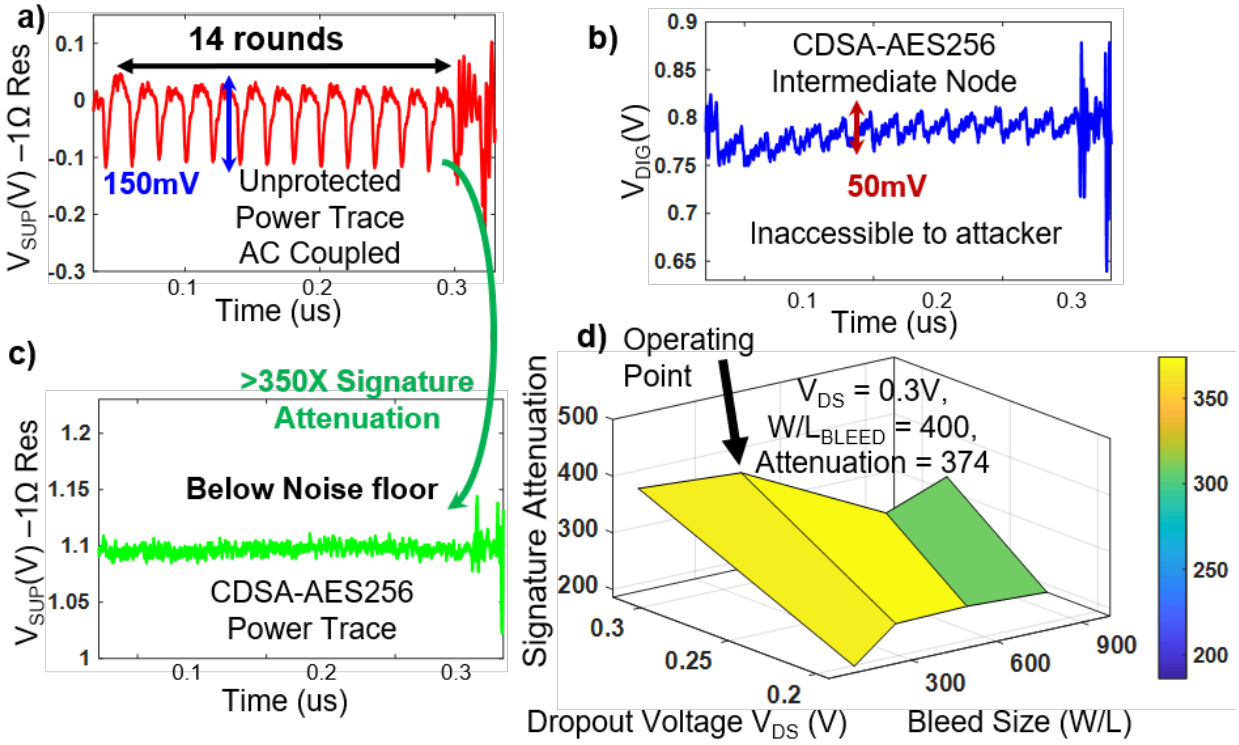


Figure 6.5. System architecture showing the circuit details of the cascode current source (CS) and the digital switched mode control (SMC) loop.

6.4 Current Domain Signature Attenuation Hardware

The main idea of the countermeasure is to embed the crypto core within the CDSA, such that the correlated current signature is significantly suppressed, and the supply current becomes almost constant (independent of the crypto current).

6.4.1 Design of the CDSA

The CDSA circuit (Fig. 6.4) utilizes digitally-tunable cascode current source (CS) with high output impedance to power the AES. The goal of the CDSA circuit is to provide an average load (AES) current plus a small delta current that leaks through the bypass PMOS bleed path to ground, providing local negative feedback leading to the ability to support any $I_{AES_{avg}}$ in between two quantized current levels of the CS (i.e. aids in analog regulation without a high-power shunt-loop). The CS consists of 32 PMOS slices, 16 of which are turned

on nominally. The unit current ($\sim 94\mu A$) of the CS is chosen such that it is higher than the key-dependent variation in $I_{AES_{avg}}$ ($\sim 72\mu A$), so that the key-dependent information in average DC current is not transferred to supply current and is leaked by the bleed PMOS, making the design highly secure. A slow digital switched-mode control (SMC) LDO tracks and regulates the voltage across the AES (V_{DIG} between $V_{TARGET}+\Delta_+$ and $V_{TARGET}-\Delta_-$) by turning on or off the required number of PMOS CS slices. It should be noted that the SMC LDO is a low-BW loop and has a dead band of 50mV, such that it remains disengaged during steady-state operation of the CDSA-AES circuit. Two dynamic comparators compare V_{DIG} with $V_{TARGET}+\Delta_+$ and $V_{TARGET}-\Delta_-$ respectively, and a 32-bit up-down counter with averaging (to control the loop frequency) controls the appropriate number of CS slices to be turned on.

Unlike traditional series LDOs, the supply current in CDSA does not track the AES current. Instead, we choose to tolerate the 30-50mV voltage droop across the AES engine (V_{DIG} is guard-banded to ensure no performance degradation at the cost of some power overhead), and the high impedance ($r_{ds} > 10K\Omega$) CS on top ensures that the current fluctuation at the supply is attenuated by $AT = \omega_{AES} C_L r_{ds}$, i.e. $> 350\times$ ($\mathrm{i}_{CS} = \frac{v_{DIG}}{r_{ds}}$, $v_{DIG} = \frac{\mathrm{i}_{AES}}{\omega C_L}$, $AT = \frac{\mathrm{i}_{AES}}{\mathrm{i}_{CS}} = \omega_{AES} C_L r_{ds}$). The use of cascode CS biased in subthreshold saturation increases r_{ds} by $\sim 10\times$ compared to one-stack CS, allowing $10\times$ reduction in C_L (only 150pF, iso-attenuation) across the crypto engine.

subsectionTime-Domain Measurement Results & Design Space The shunt path PMOS bias (near-threshold operation) as well as number of PMOS legs ON are scan controllable to analyze the effect of the extra bleed current on signature attenuation. Time-domain measurements of the unprotected AES vs. CDSA-AES show a signature attenuation of $> 350\times$ for the power traces (Fig. 6.5). Design space exploration of the CDSA-AES reveals the optimal operating point at dropout voltage of 0.3V across the CS stage and a bleed size of 400. The unprotected AES is powered with 0.8V input and consumes $\sim 1mA$ average current at 50MHz (refer Fig. 6.5(b)).

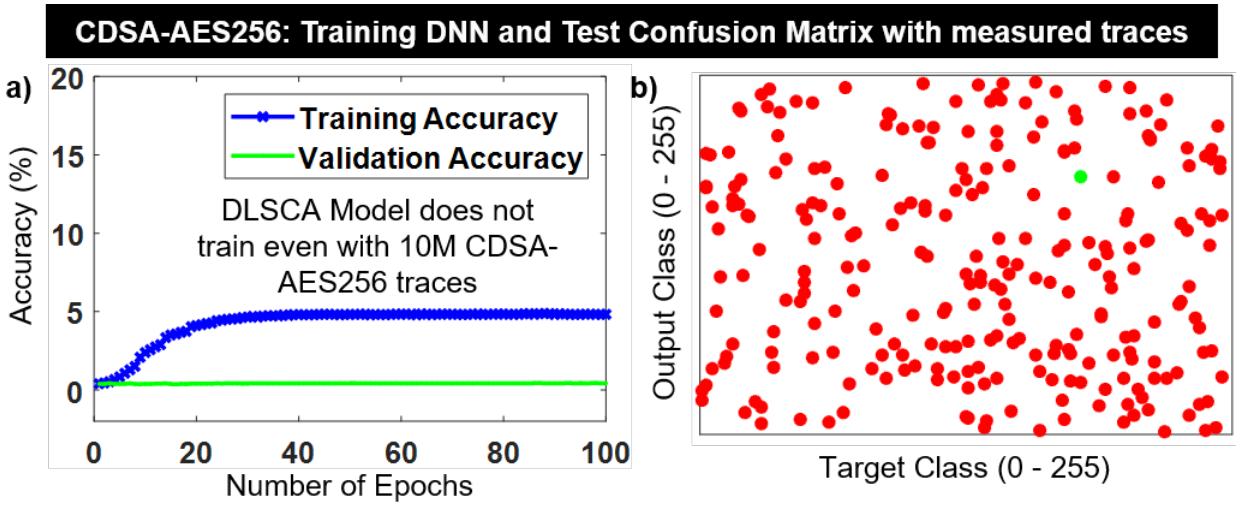


Figure 6.6. DLSCA attack on the CDSA-AES: (a) Training/validation accuracy does not improve even with $10M$ traces. (b) Test confusion matrix shows a random trend (0.3% test accuracy) with numerous misclassifications.

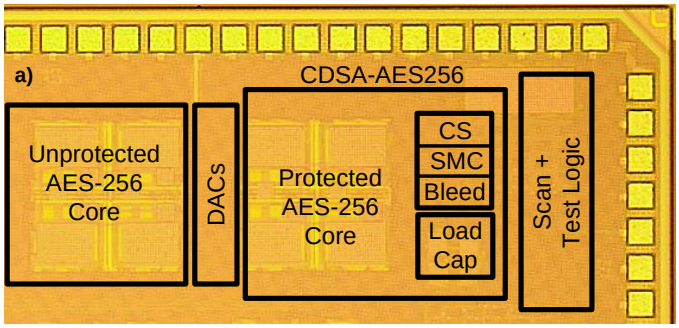
6.5 DLSCA Attack on the Protected CDSA-AES256

The captured traces from the CDSA-AES256 are now fed to the 256-class DNN for profiling. Fig. 6.6(a) shows that the DNN does not train on the protected traces (even with $10M$ traces and 100 epochs) as the signature remains deeply buried under the system noise (without any additional noise injection). Fig. 6.6(b) shows the confusion matrix for the unseen test traces from the CDSA-AES256. As we would expect, the DNN does not classify the key bytes correctly (red dots represent misclassifications) and the accuracy is close to random ($\sim 0.3\%$).

6.5.1 Comparison with the State-of-the-Art Countermeasures

Fig. **??**(c) shows a comparison with the state-of-the-art existing circuit-level countermeasures. While none of the existing countermeasures have been evaluated against DLSCA attacks, CDSA is the first circuit-level technique demonstrating DLSCA resilience.

Compared to the unprotected AES256 implementation, the DLSCA immunity is significantly improved by $> 2000\times$ ($> 10M$ compared to $5K$ traces for training), at the expense



b)		
Unprotected AES-256 Core	Performance	0.8V/50MHz/0.8mW
	Architecture	256b parallel AES
	Active Area	0.15 mm^2
CDSA-AES256	Input	1.1V
	Active Area	0.205 mm^2
	Current Efficiency	91.74%@1mA load (90uA through bleed)
	Load Cap	150pF MOS Cap (0.015 mm^2)

c) Parameter			This Work	VLSI'15 [124]	ISSCC '09 [133]	ISSCC'17 [108]	ISSCC'19 [134]
Countermeasure Technique			Current Domain Signature Attenuation	Charge Recovery Logic	Switched Capacitor Current Equalizer	Integrated Buck Regulator	Digital LDO with randomization
Process			65nm CMOS	65nm CMOS	130nm CMOS	130nm CMOS	130nm CMOS
Crypto Algorithm			AES-256	AES-128	AES-128	AES-128	AES-128
Standalone AES Power/Frequency			0.8mW @ 50MHz, 0.8V	138mW@1.32GHz	33mW @ 100MHz	10.5mW @ 40MHz	10.9mW @ 80MHz, 0.84V
Design Overheads	Area		36.7%[c]	25%	33%	1%[a]	36.9%[b]
	Power		49.8%[c]	30%	20%	5%*[a]	32%
	Perf.		0%	0%	50%	3.33%	10.4%
SCA Analysis	Time/Freq Domain		Time, Freq	Time	Time	Time, Freq	Time, Freq
	MTD/ Traces to Train	CPA	>1B (>125,000x)	940K (251x)	>10M (2500x)	>100K (20x)	8M (4210x)
		DLSCA	**>10M (>2000x)**	-	-	-	-

[a]Does not include regulator area/power, [b]Does not include MIM Cap area, [c]Power overhead includes the dropout voltage across CS, the excess bleed current drawn during the steady-state operation, as well as the V_{DIG} guard-banding to ensure no performance degradation. Area overhead includes the load cap area, CS, SMC loop, and the bleed path.

Figure 6.7. (a, b) Chip Micrograph and design summary of the system. (c) Comparison with state-of-the-art countermeasures.

of 49.8% power and 36.7% area overheads. It should be noted that the countermeasure is generic and can be extended to any other crypto engine without any performance overheads.

6.6 Remarks & Conclusion

The system developed in 65nm CMOS embeds the crypto core (AES256) within a CDSA hardware such that the critical signature is highly attenuated, to thwart DLSCA attacks. The DNN model which was trained within 5K traces for the unprotected AES256, could not be trained even with 10M traces for the CDSA-AES. The $> 350\times$ signature attenuation of the CDSA promises an improvement of $> 350^2\times$, which implies protection up to $> 600M$

traces for the DNN training. However, being limited by our capture framework for DLSCA, we could demonstrate DLSCA resilience up to $10M$ traces. Note that a fully connected DNN is chosen for the DLSCA attack as the traces are perfectly aligned in time (using the on-chip trigger pulses for end of encryption), and hence CNN is not necessary. Also, for the CDSA, signature attenuation is fundamental to the correlated leakage and hence CNNs would not provide any extra benefit over fully connected DNNs for low SNR scenarios. Although the assumption of a fixed plaintext for profiling the DNN may not be most practical for a real attack, it provides a methodology for fast leakage assessment in the machine learning domain. Finally, CDSA is a low-overhead technique to provide high resilience against DLSCA attacks ($> 2000\times$) without any performance degradation and can be extended to any other crypto algorithm.

Till now, we have focused on secure computation. In the next chapter, we will look into secure communication systems, specifically for the body area networks (BANs). We will analyze the EM physical security of the EQS-HBC communication system and compare against the traditional WBANs.

7. PHYSICAL SECURITY OF HUMAN BODY COMMUNICATION

Most of the materials in this chapter have been extracted verbatim from the paper:
1. Debayan Das, S. Maity, B. Chatterjee, S. Sen, Enabling covert Body Area Network using Electro-quasistatic human body communication, *Scientific reports, Nature*, 2019.

Radiative communication using electro-magnetic (EM) fields amongst the wearable and implantable devices act as the backbone for information exchange around a human body, thereby enabling prime applications in the fields of connected healthcare, electroceuticals, neuroscience, augmented and virtual reality. However, owing to such radiative nature of the traditional wireless communication, EM signals propagate in all directions, inadvertently allowing an eavesdropper to intercept the information. In this context, the human body, primarily due to its high water content, has emerged as a medium for low-loss transmission, termed human body communication (HBC), enabling energy-efficient means for wearable communication. However, conventional HBC implementations suffer from significant radiation which also compromises security. In this article, we present Electro-Quasistatic Human Body Communication (EQS-HBC), a method for localizing signals within the body using low-frequency carrier-less (broadband) transmission, thereby making it extremely difficult for a nearby eavesdropper to intercept critical private data, thus producing a covert communication channel, i.e. the human body. This work, for the first time, demonstrates and analyzes the improvement in private space enabled by EQS-HBC. Detailed experiments, supported by theoretical modeling and analysis, reveal that the quasi-static (QS) leakage due to the on-body EQS-HBC transmitter-human body interface is detectable up to $< 0.15m$, whereas the human body alone leaks only up to $\sim 0.01m$, compared to $> 5m$ detection range for on-body EM wireless communication, highlighting the underlying advantage of EQS-HBC to enable covert communication.

7.1 Background

Future advancements of societally critical applications such as connected healthcare, electroceuticals, neuroscience, augmented and virtual reality rely on small form-factor wearables [135], [136], implantables, injectables, ingestibles, and other on-body internet-connected devices, triggering the need for energy-efficient and secure mechanisms for information exchange [137]. This trend has transformed the human body to an integrated network of electronic devices that includes biomedical sensors, closed-loop neuromodulation systems, smartwatches, glasses, or even mobile phones. Wireless Body Area Network (WBAN) has been the de-facto standard for connecting these tiny energy-sparse devices. However, wireless communication using EM fields is fundamentally radiative and attenuates in power density as it propagates through space. Due to this radiative nature of WBAN, the signals require high transmission power and they propagate in all directions. These EM emanations can be easily intercepted by any malicious eavesdropper, who wants to gain access to the critical private information. Hence, data encryption becomes necessary in case of wireless communication. However, such information-theoretic secrecy do not mitigate the threat to user's privacy [138] from the very existence of the message itself. Moreover, even the most theoretically robust cryptographic algorithm can often be defeated by an adversary using non-computational techniques such as side-channel analysis.

Quite recently, bio-physical communication using the human body has gained prominence as an energy-efficient information exchange modality [139], [140], as the high-water content of our body provides a low-loss channel for signal propagation. Human Body Communication was first proposed as a method to connect devices on a Personal Area Network (PAN) by Zimmerman et al. [141]. Both the transmitter and the receiver are electrically isolated and battery powered devices. The transmitter capacitively couples a narrowband signal on the surface of the human body creating electric fields and the displacement current is picked up at the receiver [142], [143]. The closed loop path is formed by the capacitive coupling between earth's ground and ground electrode of the devices [144], [145]. Due to the capacitive return path, this mode is often referred to as capacitive HBC. Oberle [146] and Wegmueller et al. [147] investigated galvanic coupling in which the signal is applied between

two electrodes of the transmitter in direct contact with the human body, and the potential difference generated by the induced electric fields from signal source is sensed by the receiver electrodes on other side of the body. Such differential excitation and termination mode is commonly referred to as galvanic HBC. In the case of galvanic coupling, most of the current flows between the two electrodes of the transmitter device, as it forms a low resistance path for the induced electric current. This increases the loss in galvanic coupling as the distance between the transmitter and receiver increases, making galvanic HBC unsuitable for long-distance on-body communication from a small transmit device [55]. Based on these two types of HBC, there have been several studies characterizing the channel loss and signal transmission mechanisms for intra-body HBC [148], [149]. Analysis of EM wave interactions with the human body has also been extensively studied [150], [151], [152], [153].

However, most previous efforts have been focused on narrowband human body communication (NB-HBC). NB-HBC couples modulated narrowband EM signals (20-80 MHz carrier frequency) to the human body using a coupler instead of radiating it with an antenna. The energy consumption of traditional WBANs is in the order of $\sim$ 10 nJ/bit [154], whereas NB-HBC techniques consume $\sim$ 110 pJ/bit [155]. We have recently demonstrated that broadband HBC could reduce this energy-efficiency to $<$ 10 pJ/bit [156], [8], [9], [157], [11], [158]. It implies that for a mm^3-sized battery with 2 J of available energy, WBAN can only support $\sim$ 2 sec of data transfer at a data rate of 100 Mbps, whereas a HBC enabled device can support up to $\sim$ 2000 sec for the same data rate. Although NB-HBC is more energy-efficient than WBAN, the EM nature of communication radiates significant amount of signal outside the body, thus not maintaining the data privacy.

In this work, we present a private body area network utilizing Electro-Quasistatic (EQS) transmission to enable physical-layer covert and secure communication. EQS-HBC uses electro-quasistatic signal transmission through the conductive layers below skin, and capacitive return paths with carrier-less signals at frequencies below 1 MHz. As shown in Fig. 7.1, EQS-HBC couples the carrier-less signals through skin layer to the conductive layers below the skin. The coupled signals create an electro-quasistatic (EQS) field throughout the body and the potential difference thus created can be picked up by wearables and implantables distributed around the body. Privacy is essentially enabled by a combination of electro-

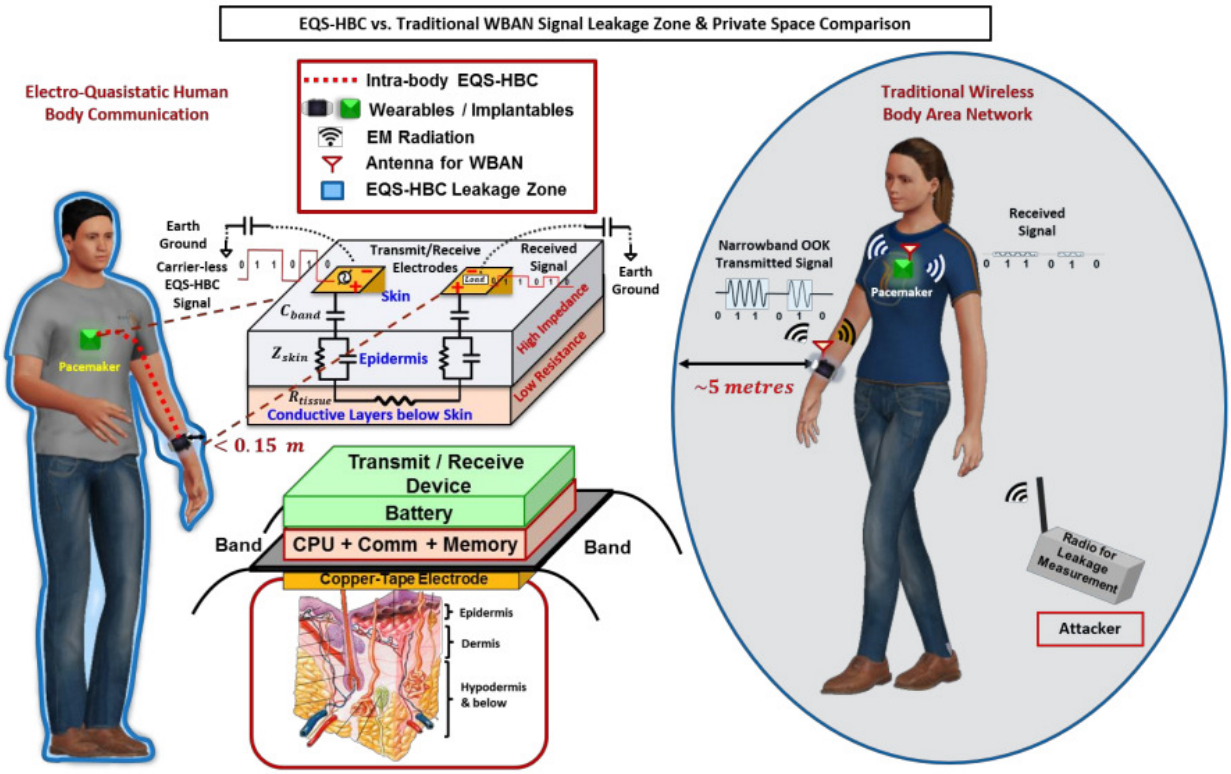


Figure 7.1. EQS-HBC vs. WBAN: An Overview of the Data Privacy Space. Persons wearing transmitter device (pacemaker) and an on-body hub communicating using EQS-HBC (left) and WBAN (right) respectively. For the intra-body EQS-HBC, signals are coupled to the surface of the human body using an interfacing copper electrode which protrudes from beneath the transmitter consisting of communication module, processing module, memory, and power source. The transmitted signal flows through the low resistance layers of the body below the skin and is picked up by the receiver electrode. On the other hand, WBAN uses an antenna to radiate the signals wirelessly up to a larger distance that can be picked up by a nearby eavesdropper. The privacy space in case of EQS-HBC (< 0.15 m) is significantly improved by an order of $> 30\times$, compared to WBAN ($\sim$5 m). The human figures were created using the open-source software 'MakeHuman'[159]. The detailed anatomy of the human skin layer structure can be found in [56].

quasistatic nature of signals involved, ensuring communication signals are not radiated out, along with signal transmission through the conductive layers below the skin, which ensures critical signals stay mostly within the body. Here we use EQS-HBC to reduce signal leakage, making the physical signals hide under ambient noise from a nearby attacker's perspective, enabling covert communication.

We observe that carrier-less EQS-HBC data transfer maximizes the information capacity of the channel compared to the narrowband signaling (NB-HBC), as it utilizes the full bandwidth instead of a fractional-bandwidth around a carrier frequency. Correspondingly, to achieve the same data rate, wireless signals as well as NB- HBC need to choose a high enough carrier frequency (f_c) so that the fractional BW at that frequency equals the EQS human body communication capacity. The high f_c leads to higher EM leakage and hence NB-HBC lacks the inherent physical security. Data security and privacy is a critical aspect for most human-centered applications including wearable medical devices used for patient monitoring [57], [54], e.g. a doctor reprogramming a pacemaker using the patient's smartwatch. If the wireless data transmissions can be confined within the human body, it would enable a form of physical-layer covert and inherently secure communication that is currently non-existent on wearable and implantable devices. EQS-HBC presents itself as a strong candidate for enabling covert communication and this work explores the security and privacy aspects of EQS-HBC. Although the magnetic fields are very weak due to the electro-quasistatic nature of transmission, an external eavesdropper can try to detect the quasi-static (QS) leakage (QSL). This work presents various experiments in both time and frequency domains using custom-designed EQS-HBC device, supported by theoretical leakage-models to analyze this side-channel QS leakage, and demonstrates the privacy and security of human body data transmission using EQS-HBC.

7.2 Electro-Quasistatic Human Body Communication (EQS-HBC): Fundamentals

EQS-HBC uses electro-quasistatic transmission through the conductive layers below skin, and capacitive return paths with carrier-less signals at frequencies below 1 MHz.

7.2.1 Signal transmission through Conductive layers below Skin

In this work, the signals are capacitively coupled to the epidermal skin layers of the human body which then flows through the conductive layers below of the skin and is finally picked up capacitively at different on-body receivers. The magnitude of the skin impedance

(Z_{skin}) typically varies in the range of $1K\Omega - 100K\Omega$, depending on the condition of the skin, presence of moisture and other factors [160], [161], whereas the lumped resistance for the layers (R_{body}) is $\sim 100 - 400\Omega$[160], [161], [162].

7.2.2 Electro-Quasistatic Data Transmission

For both capacitive as well as galvanic coupling, the potential difference created by the magnetic fields is ignored since no closed coupling loops exist at the transmitting or receiving electrodes. Hence, below a certain frequency (f) limit, magnetic fields would not contribute in the data transfer allowing electro-quasistatic (EQS) through the human body. The ratio between the magnitudes of the developed electric field ($\vec{E}$) and the approximation error ($\vec{E}_{error}$) in the case of EQS transmission is given as [163], [164]:

$$\vec{E} = \vec{E}_{EQS} + \vec{E}_{error}, \frac{E_{EQS}}{E} = \omega^2 \mu \epsilon {r_{tx}}^2 \tag{7.1}$$

In Eqn. 7.1, r_{tx} represents the dimension of the transmit device for EQS-HBC ($r_{tx} \sim 0.02$ m, refer to Methods Section), ϵ and μ denotes the permittivity and permeability, respectively, of the medium (conductive tissue layer of the human body, in this case). The maximum relative permittivity (for the worst case) of the tissue layers of the human body is 3000. The nearfield quasi-static approximation ($\vec{E} \approx \vec{E}_{EQS}$) holds good as long as the magnitude of $E_{error} \ll E$, which implies:

$$\omega^2 \mu_{tissue} \epsilon_{tissue} {r_{tx}}^2 \ll 1, \epsilon_{tissue} \approx 3000 \epsilon_{air}, \mu_{tissue} \approx \mu_{air} \tag{7.2}$$

$$f_{EQS-HBC} \ll \frac{1}{2\pi r_{tx} \sqrt{\mu_{tissue} \epsilon_{tissue}}} \approx 43.61 MHz \tag{7.3}$$

As seen from Eqn. 7.2, 7.3 [165], [166], considering $c = 3 * 10^8 m/s$ as the velocity of propagation of EM waves in air, the intensity of the electromagnetic fields radiated is

dominated by the quasi-static nearfield, as long as $f_{EQS-HBC} \ll 43.61MHz$. It should, however, be noted that biological tissue is dispersive, and the threshold frequency could vary. In this work, we employ transmission frequency of 1 MHz thereby allowing quasi-static field (approximation error $= (\frac{1MHz}{43.61MHz})^2 * 100 = 0.05\%$) as the dominant mode of propagation through the body and thus enabling electro-quasistatic human body communication (EQS-HBC).

On the other hand, for the EQS-HBC leakage, considering the human body as an antenna (maximum height of the human body r_{body}<2 m), and that the leakage signal out of the human body is being picked up in the air medium (ϵ_{air}=1), the threshold frequency evaluates to $f_{QSL} \ll 23.88MHz$. This yields an approximation error of $\sim 0.2\%$ for the quasi-static assumption of the leakage signal at 1 MHz.

7.2.3 Steganographic Covert Communication

Steganography is a form of covert communication which hides the transmitted data from a third party even without encryption. In the context of wireless communications, spread spectrum techniques to hide information in channel noise have been explored which comes at the expense of extra communication energy [167]. Analogously, while the EQS-HBC transmitted signals suffer low loss, the leaked EQS-HBC signals are concealed within noise for an attacker, thereby showing promise to enable covert steganographic communication in the form of an inherent physical layer security.

7.3 EM Radiation in WBAN and Side-channel Quasi-Static Leakage in EQS-HBC

In traditional WBANs, the transmitter radios are designed to transmit data wirelessly as far as possible over air, instead of restricting the transmission to the body, which makes it inherently insecure. Even in presence of encryption, there have been several vulnerabilities of different radio protocols for wearable and implantable devices [159].

In the case of EQS-HBC, although the transmitted broadband signal suffers loss due to the weak capacitive return path between the transmitter and the receiver [56], [168], the

loss is significantly lower than wireless signal propagation. Hence the received signal can be reliably decoded by an interference-robust receiver [169], [53], [170], [171]. From the security perspective of EQS-HBC, if it can confine the data transmission within the human body, it would enable a form of physical layer security, which is presently non-existent in WBANs. Thus, the data transmission would be fully secure from an external malicious attacker. The adversary needs to be in direct physical contact with or be almost touching the person to gather any EQS-HBC data. This will enable secure and covert communication without any overhead, with orders of magnitude lower energy than WBAN, which is currently non-existent. EQS-HBC introduces a basis for physical security. An additional layer of mathematical security (i.e. encryption) may or may not be added depending on the application scenario and trust factors, e.g. if it can be ensured that an adversary cannot touch the human without his/her knowledge during EQS-HBC, no additional encryption will be necessary.

To evaluate the inherent data security and privacy of the EQS-HBC transceiver system, we need to analyze whether any signal in the form of quasi-static field "side-channel" is being leaked from the human body during EQS-HBC. Fig. 7.1 provides an overview of the private space for EQS-HBC and WBAN in the presence of an external adversary who can detect the leaked ('radiated' in the case of WBAN) QS signals and can attempt to obtain the critical information [55], [49].

A series of experiments in time and frequency domain are performed to determine this critical leakage during EQS-HBC. The methods are elaborated along with the experiments and results.

7.4 Results

The main goal of performing the experiments is to analyze if the body itself leaks information during the electro-quasistatic human body communication (EQS-HBC). As discussed earlier, capacitive EQS-HBC shows lower channel loss than the galvanic HBC over long distances in the body, and hence our experiments are with capacitive EQS-HBC. The EQS-HBC transmit device (Fig.7.1) is built using off-the-shelf components, and consists of a communi-

cation module, processing module, memory, power source, and an interface with the human body. The details of the set-up and the EQS-HBC transmit device are discussed in the Methods section. An interfacing band consisting of copper electrode couples the transmitted signals into the body. The received EQS-HBC signal and the QS leakage (QSL) is then measured from other parts of the body using antenna or voltage probes as appropriate, and the probing positions are specified for individual experiments. It should be noted that in a few experiments, QS leakage is reported with direct probe contact (d=0), which is to demonstrate the value of leakage at the source of the leakage signal.

7.4.1 Time-domain correlational analysis of QS Leakage Signature

In this experiment, the goal is to examine if any QS leakage can be detected during EQS-HBC data transmission.

As shown in Fig. 7.2, the EQS-HBC transmit electrode is coupled to the human forearm (device arm). The transmitter (microcontroller) is excited with a pseudo-random binary sequence (PRBS) at 1 MHz, and using an oscilloscope and a telescopic antenna, the auto-correlation (ρ) between the known PRBS data sequence and the QSL signal is measured with varying distances (d) away from the body and two angles ($\theta = 0°$: parallel to the antenna, $\theta = 90°$: perpendicular to the antenna) between the device hand and the antenna, as shown in Fig.7.2(a). Next, the QS leakage from the free hand is measured with varying distances between the free hand and the antenna connected to the oscilloscope (Fig.7.2(b)).

Correlational analyses for the QS signals leaked during EQS-HBC from the device hand and the free hand respectively, are shown in Figure 2(c, d). From Figure 2(c), it can be seen that although the QS leakage from the hand with unshielded EQS-HBC device is detectable up to 0.5 m, EQS-HBC signals contained in the free hand does not leak beyond 0.01 m, although both the hands contain the same amount of EQS-HBC signal (Fig. 7.3 – green curve).

The above observations prove that the human body itself does not leak, but the EQS-HBC transmitter is the source of the QS leakage. However, this experiment does not provide conclusive proof if the transmitter itself leaks the signals.

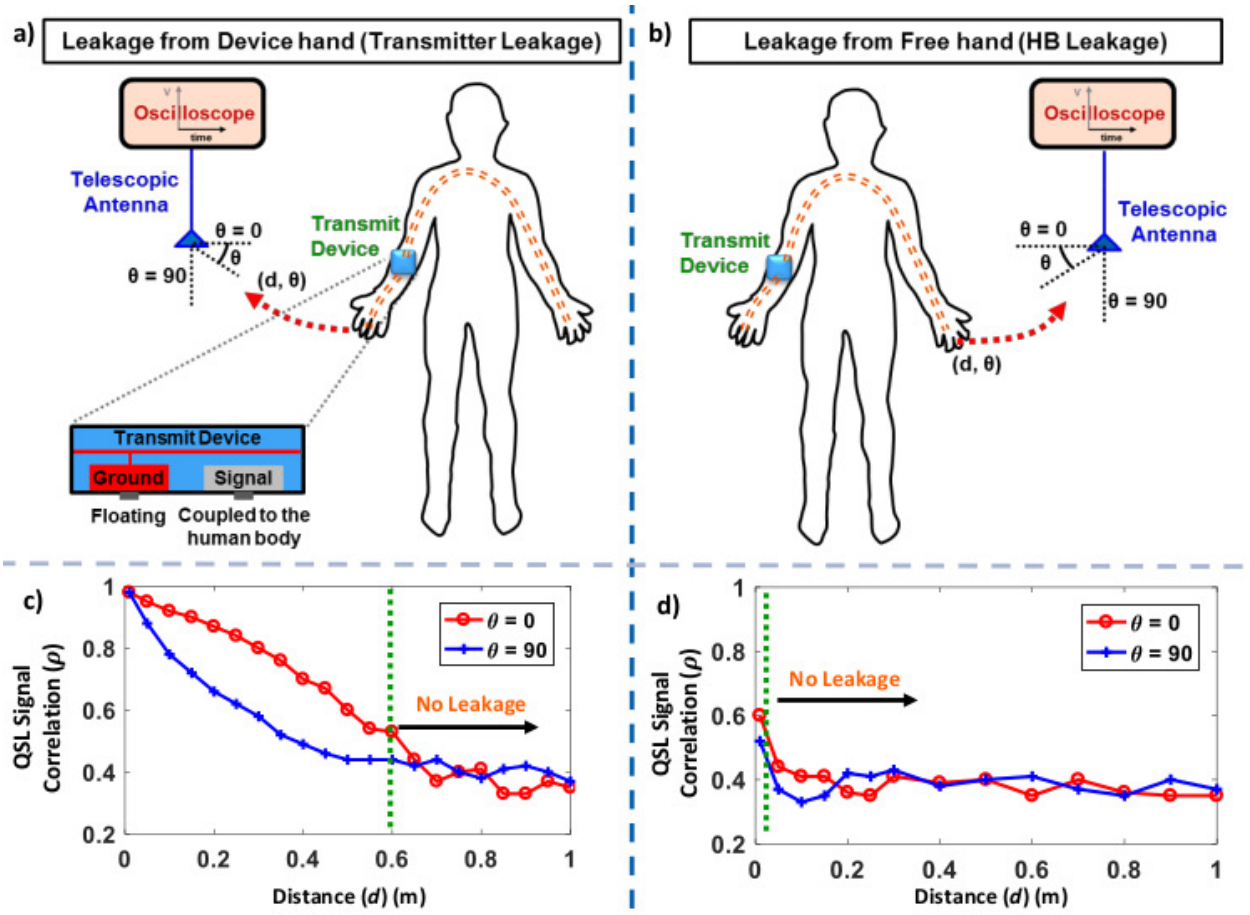


Figure 7.2. Time-domain Measurements of capacitive EQS-HBC Quasi-static Leakage (QSL) using Oscilloscope with the transmitter wearable device on the device arm. (a, b): Simplified experimental set-ups to measure the QS leakage from the device and free hands respectively; (c, d) Voltage Correlational analysis of the measured QS leakage for the device and free hands respectively, with varying angles (θ) and distances (d) between the antenna and the hands. The measured QS leakage from the device hand is dominated by the leakage due to the EQS-HBC transmitter, while the free hand leakage corresponds to QS leakage due to the human body (HB) alone.

7.4.2 Time-domain Measurements of EQS-HBC Received Signal and the QS Leakage Signature

In this experiment, the goal is to check whether both the device hand and the free hand contains the same amount of signal, and also that the EQS-HBC signals are transmitted through the human body and not through the air.

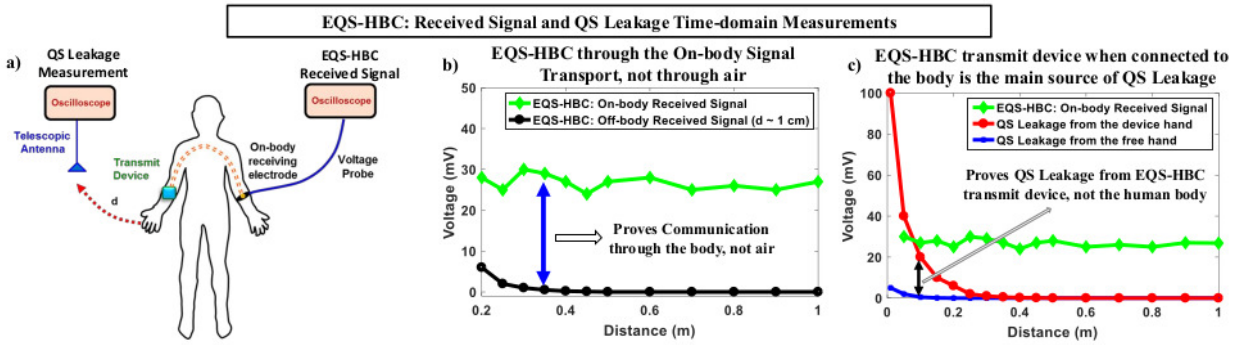
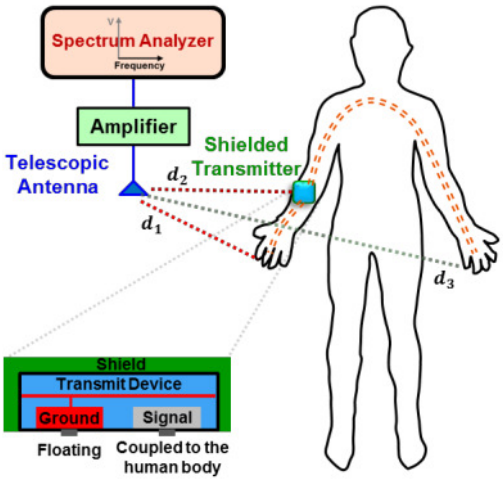


Figure 7.3. EQS-HBC Signal Transmission ($V_{EQS-HBC}$) and Quasi-static Leakage (V_{QSL}) Signal Measurement with distance in time-domain using an oscilloscope, voltage probe, and an antenna. The transmission signal amplitude is 3.3 V. (a) EQS-HBC Received signal at different on-body locations is ∼30 mV (green curve) showing a channel loss of ∼40 dB which is almost independent of the distance between the transmitter and receiver. Off-body signal corresponding to each of the human body receiver locations is measured in air with very close proximity from the body ($d_{off-body} \sim 0.01$ m) (black curve). This shows that the EQS-HBC occurs through the on-body signal transmission, and not through the air. (b) The EQS-HBC signal received at different locations of the body is ∼30 mV (green curve). Quasi-static Leakage around the body is measured in air medium from both device hand (red curve) and free hand (blue curve) respectively. The QS leakage (QSL) measurement set-up is shown in Fig. 4.10. Note that for the EQS-HBC received signal measurement, distance refers to the on-body distance between the transmit device and the receiving electrode. In the case of leakage measurements here, it is the distance between the antenna and the corresponding hand for which the leakage is measured. The free hand, although contains almost the same amount of signal, leaks considerably lesser than the device hand, proving that human body alone does not leak. However, the human body aids the transmit device to leak (device hand leakage) by providing a low impedance closed path with the earth ground, which will be discussed in the next experiments.

The received EQS-HBC signal in different locations (varying distances) on the body is measured, as shown in Fig.7.3(a) (green curve). Corresponding to each on-body location, the off-body quasi-static (QS) leakage is also measured in very close proximity ($d_{off-body} \sim 0.01m$) to that location. Fig.7.3(a) shows the amount of received signal for EQS-HBC is almost independent of the distance between the transmitter and the receiver, which is expected in capacitive human body communication. The off-body signal measured in air at very close proximity corresponding to each of the receiving location is very small compared



Modes		Power (dBm)
Leakage from Unshielded Standalone Transmitter ($d = 0^+$)		-40
Leakage from Shielded Standalone Transmitter ($d = 0^+$)		*Below NF* < -90
EQS-HBC With Shielded TX	Direct antenna touch with device hand – EQS-HBC received power ($d_1 = 0$)	-54
	Direct antenna touch with free hand – EQS-HBC received power ($d_3 = 0$)	-60
	QS Leakage – EQS-HBC Transmitter (worn) very close to antenna ($d_2 = 0^+$)	-48
	QS Leakage – Free Hand very close to antenna but not touching ($d_3 = 0^+$)	*Below NF* < -90

Figure 7.4. Spectrum Analyzer Measurement shows that the shielded standalone transmitter does not radiate. However, the transmitter when worn on the human body for EQS-HBC shows significant leakage (-48 dBm). Note that for the capacitive EQS-HBC, although both the device and free hands contain similar amount of signal (-54 dBm,-60 dBm respectively), the free hand shows negligible QS leakage ($< -90dBm$).

to the on-body received signal. This clearly shows that the EQS-HBC communication is established through the low-loss on-body signal transmission and not through the air.

This experiment (Fig.7.3(b)) shows that the QS leakage from the device hand (red curve) is considerably higher than the free hand (blue curve), which is consistent with the correlational analysis from the previous experiment (Fig.7.2). This is a very fascinating observation since both the hands contain almost the same amount of EQS-HBC signal (Fig.7.3(a) - green curve).

Another important point to note from Fig.7.3(b) is that although at very small distances, the leakage measured is high, the on-body signal measured remains at the same level. This is because of the weak capacitive return path in case of EQS-HBC communication.

7.4.3 Shielded Standalone Transmitter QS Leakage

From the previous experiments, it is evident that the EQS-HBC transmitter leaks. This goal of this experiment is to investigate whether the standalone transmitter leaks by itself, that is, without the human body connected to it.

To perform this measurement, the effect of the connected wires needs to be eliminated. Hence, the transmitter is shielded using a copper-coated box forming a Faraday cage, with the shield (Sh) (refer to the circuit modeling sub-section) connected to a fixed potential. The shield thus hides the ground plane (N) of the EQS-HBC transmitter from coupling directly to the Earth ground (low coupling capacitance C_{gn}), thereby ensuring that the effect of QS fields emanating from the transmit device and the connected wires are eliminated. However, since the shield needs to be connected to a fixed potential, the transmitter ground (N) is connected to the shield, which now forms a capacitive path (C_{gsh}) with the earth ground. Without any contact with the human body, the standalone transmitter device is powered on with a 1 MHz PRBS signal, and the leakage from the device is measured using a spectrum analyzer (SA) and an antenna connected through a wide-band amplifier. It should be noted that SA provides a low impedance termination (50Ω) and hence both the EQS-HBC received power and the quasi-static (QS) leakage power measured is less. However, it provides a fair comparison for different measurement modalities and to root-cause the source of the QS leakage during EQS-HBC. We can expect that if the shielded transmitter without EQS-HBC shows high QS leakage, it can be concluded that the standalone transmitter itself leaks.

As seen from the table in Figure 7.4, the unshielded standalone transmitter leaks significantly (-40 dBm), when in close proximity to the antenna ($d = 0^+$), whereas the shielded transmitter shows negligible signal leakage (below noise floor: <-90 dBm at $d_3 = 0^+$)

The above observations confirm that the shielded standalone transmitter does not leak any QS signal.

7.4.4 Shielded Transmitter Leakage during EQS-HBC

The goal of this experiment is to examine whether the shielded transmitter in contact with the human body causes the quasi-static leakage during EQS-HBC data transmission.

The shielded transmitter is worn on the forearm (device arm) for EQS-HBC. Using the same set-up as in experiment 3 (Fig.7.4), with the SA and the antenna, the signal level for the case of direct contact with the device hand ($d_1 = 0$) and the free hand ($d_3 = 0$) is measured respectively. It can be seen from Fig.7.4 that the signal power contained as measured in the SA is -54 dBm in the device hand and -60 dBm in the free hand. As expected, the path loss is lower for capacitive mode, and both the hands contain similar amount of the EQS-HBC signals. As the EQS-HBC transmitter on the device hand is brought in close proximity to the antenna ($d_2 = 0^+$), the QS leakage is significant (-40 dBm), as seen from Fig.7.4. Another fascinating observation is the fact that the signal contained in the free hand (-60 dBm) immediately dies down (below noise floor of the SA) within a few mm, as the leakage signal power measured from the free hand at close proximity of the antenna ($d_3 = 0^+$) is negligible (below noise floor: $< -90dBm$). The above observations from this experiment confirm that even after shielding, the transmit device when connected to the human body causes the QS leakage.

From the above experiments, it is clear that neither the human body alone, nor the transmitter itself leaks the signals. However, the EQS-HBC transmitter (even after shielding) in contact with the human body shows leakage.

7.4.5 EQS-HBC Quasi-Static Leakage Field Distribution

The goal of the field distribution analysis (Fig.7.5) is to explain the basis behind the observations in previous experiments for different configurations of the transmit device.

Fig.7.5(a, b) shows the electric field distributions due to the standalone transmitter device without any body contact. For mode 1, in absence of the measuring probe (no nearby attacker) and without the human body, the closed path from the small 'Signal' plate of the transmitter to the Earth ground is formed by a very weak coupling capacitance (C_{gs}). Hence the fields formed between the signal terminal and the Earth ground are very weak, and

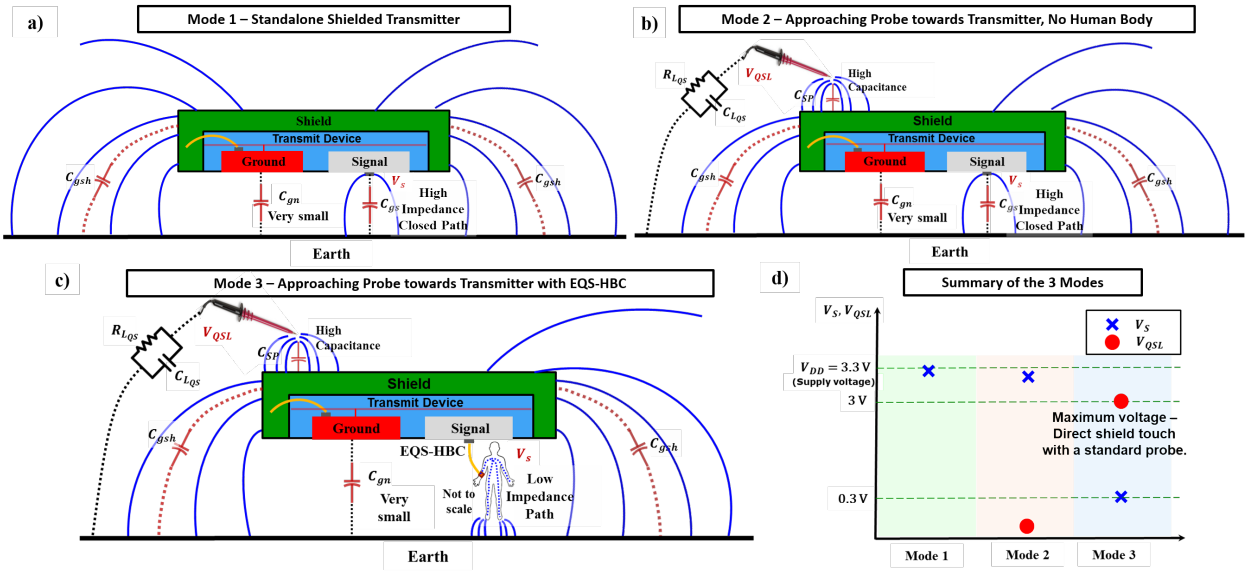


Figure 7.5. QS Field distributions for different configurations of the transmitter device. (a) In mode 1, voltage drop across the signal plate of the Standalone shielded transmitter and earth ground is maximum ($V_S \sim V_{DD}$) as there is no direct path from the signal plate to the earth ground. (b) In mode 2, as an attacker approaches with a probe towards the shielded transmitter, it receives negligible voltage as no current flows due to the high impedance path from signal to ground. Hence, standalone shielded transmitter does not leak. (c) In mode 3, Human body coupled to the transmitter device for EQS-HBC provides a low resistance closed path to ground; hence higher voltage received by the attacker (V_{QSL}) (d) Summary of the 3 modes – In absence of the human body, all the voltage drop (V_S) occurs across the signal terminal and ground and the attacker does not pick any signal (mode 2). In presence of the human body, a close-by attacker (touching the shield) can obtain a high signal. Hence, in spite of shielding, the EQS-HBC transmitter device leaks.

significant portion of the transmitted signal voltage drop occurs across the Signal plate and the Earth ground ($V_S \approx V_{DD}$, Supply Voltage). As an attacker approaches to intercept the data being transmitted, the probe forms a low impedance path between the shield (connected to the ground terminal of the transmitter) and the Earth ground. However, the signal plate to the Earth ground still presents a high impedance path, and most of the signal still drops across C_{gs}, i.e. $V_S \leq V_{DD}$. Hence the attacker can only receive negligible amount of signal $V_{QSL} \approx 0$.

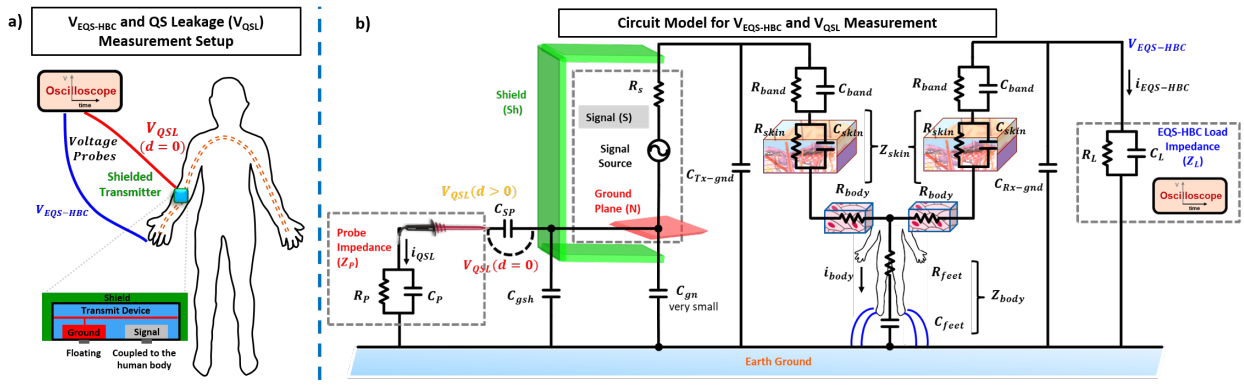


Figure 7.6. (a) EQS-HBC Measurement set-up with the shielded transmitter in the wrist (device arm) and (b) its corresponding circuit model. The impedances for the skin and tissue layers [54] are modelled, along with the signal sources, copper electrode coupler (band) and the measurement probes, to form the complete circuit model for EQS-HBC. Note that the probe is directly connected (d = 0) to the human body to measure the signal level from the source of the leakage. The EQS-HBC received voltage is measured from the fingers of the device hand.

Fig.7.5(c) analyzes the field distributions due to the transmitter device during EQS-HBC data transmission in presence of the probe (emulating an attacker). In mode 3, the human body forms a low resistance path between the small Signal plate to the Earth ground which now allows current to flow. In this case, the attacker obtains the maximum amount of the transmitted signal $V_{QSL} \sim 3V$, using voltage probes with an oscilloscope with high termination impedance ($10M\Omega$).

The above analyses infer that the human body alone does not leak, and the shielded standalone transmitter device does not radiate. However interestingly, even the shielded transmitter leaks during EQS-HBC, when in contact with the human body, which is explained through the QS field theoretic viewpoint (Fig.7.5(c)). This observation conclusively suggests that the human body is aiding the transmitter to leak information.

7.4.6 Theoretic Circuit Modelling of the EQS-HBC Leakage & Experimental Validation

The goal now is to develop a circuit model for EQS-HBC (Fig.7.6(b)) to further analyze the cause of the QS leakage and to implement countermeasures for reducing the "side-channel" leakage information.

In the case of EQS-HBC, the signal transmission is dominantly electro-quasistatic and hence the lumped circuit approximation holds (since wavelength $\lambda \sim \frac{3*10^8 m/s}{\sqrt{8}*1MHz} \sim 105m$ of the transmitted signal is much greater than the length (l$\sim 2m$) of the transmission channel, that is, human body). The different elements of the circuit model (Fig.7.6(b)) include the signal generator source resistance (R_s), the band to skin capacitance (C_{band}), skin layer resistance (R_{skin}), skin layer capacitance (C_{skin}), body resistance (R_{body}), feet to ground capacitance (C_{feet}), shield (connected to transmitter ground) to earth return path capacitance (C_{gsh}) and the load impedance due to the probes (Z_P, Z_L) for measuring the leakage and the EQS-HBC received voltage respectively. The source impedance of the signal generator $R_s = 50\Omega$. The band capacitance is formed due to the small air gap (d) between the transmitter electrode and the skin, which is in $\sim 200pF$ considering the electrode size of $\sim 0.0004m^2$ and d=0.01 mm. The skin layer resistance $R_{skin} \sim 5K\Omega$ and typically varies in the range of $1K\Omega - 100K\Omega$ [160], [161], depending on the skin moisture and other factors. The skin layer thickness is in the range of 0.1-4 mm, and considering skin area of $\sim 0.0004m^2$ near the EQS-HBC transmit device, the skin layer capacitance (C_{skin}) can be computed to be $\sim 100pF$. The body resistance (R_{body}) is in the range of $100 - 400\Omega$ [160], [162]. The resistance of the tissue could depend on the on-body transmission distance. However, it does not affect the EQS-HBC channel loss or the measured QS leakage. The feet to ground capacitance $C_{feet} \sim 10pF$, considering a feet area of $\sim 0.01m^2$ and a feet to ground separation of 0.01 m [172]. The measurement probes are modelled as the load (Z_P, Z_L respectively) for both the QS leakage and EQS-HBC received voltage signal. In this set of experiments, the shield (Sh) is connected to the ground (N) of the transmitter device.

The QS leakage and the received EQS-HBC voltage signal are measured using an oscilloscope by putting a voltage probe on the shield (direct contact) and the device hand

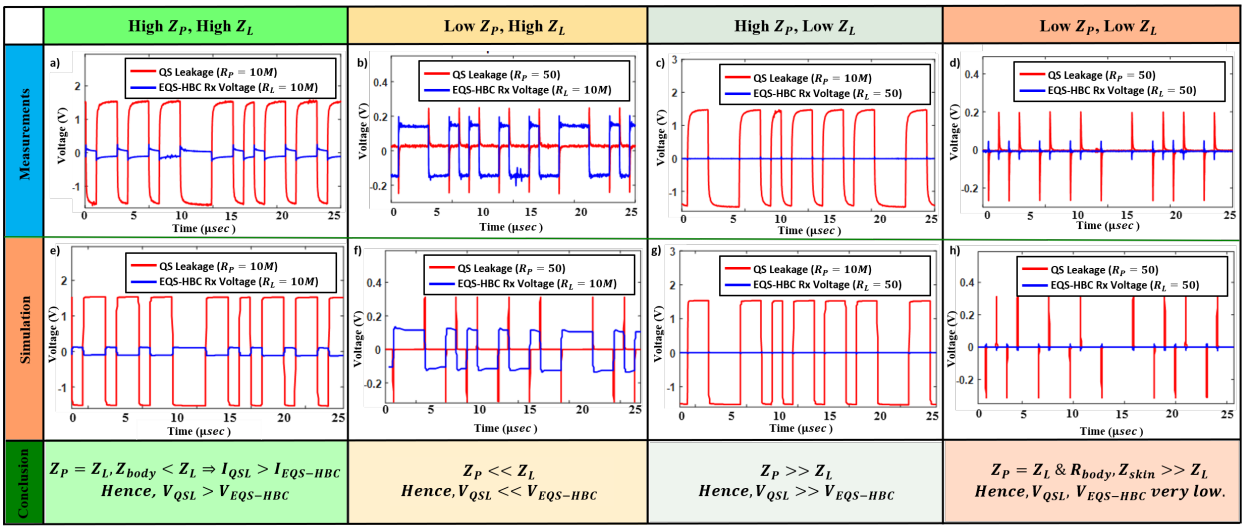


Figure 7.7. Measured oscilloscope signals with the EQS-HBC set-up shown in Fig.7.6(a), for different termination for both the QS leakage and the EQS-HBC received voltage. (e-h): Proposed Circuit Model (Fig.7.6(b)) simulation waveforms for the same set of loading constraints. The simulation results complement the actual measurements for all different conditions, proving that the model is accurate. Note that the QS signature is inverted to the actual transmitted signal.

respectively (Fig.7.6(a)). Although the shielding significantly reduces the return path capacitance between the transmitter ground and the earth ground (C_g), the shield capacitively couples to the earth's ground through C_{gsh}. Hence, shielding the EQS-HBC transmitter does not eliminate the unnecessary QS leakage, which has been demonstrated in previous experiments.

Fig. 7.7(a-d) shows the oscilloscope captured waveforms with the shielded transmitter prototype, for 4 different load combinations (2 probes each having 2 impedances: 10Ω and 50Ω), for both the QS leakage and the EQS-HBC received voltage. Note that both probes are connected for measuring the QS leakage and the received HBC voltage simultaneously. In Fig. 7.7(a), $R_P = R_L = 10M\Omega$, and, $Z_{body} < Z_L$; hence the current and voltage received by the probe is higher than the EQS-HBC current $I_{QSL} > I_{EQS-HBC}$, and $V_{QSL} > V_{EQS-HBC}$. When the probe impedance ($R_P = 50\Omega$) is significantly lower than the load impedance for EQS-HBC ($R_L = 10M\Omega$), $Z_P \ll Z_L$, hence $V_{QSL} \ll V_{EQS-HBC}$ (Fig.7.7(b)). Similarly, when the receiver EQS-HBC load impedance ($R_L = 50\Omega$) is much lower than the probe impedance

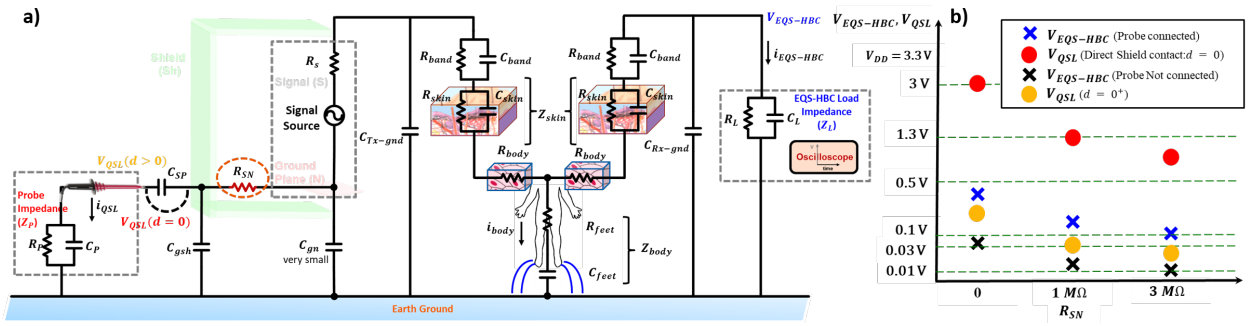


Figure 7.8. Countermeasure against EQS-HBC leakage. (a) A high resistance (R_{SN}) de-couples the transmitter ground plane and the shield. (b) EM (V_{QSL}) and EQS-HBC voltage ($V_{EQS-HBC}$) levels are measured against different values of R_{SN}. As R_{SN} is increased, both V_{QSL} and $V_{EQS-HBC}$ reduces. Beyond a certain value of R_{SN}, the EQS-HBC received signal gets reduced and can no longer be decoded. Hence, there exists an optimum between the area of the shield connected with transmitter ground through R_{SN}, and the remaining area that connects to the transmitter ground directly, so as to minimize the EM leakage while maintaining reliable EQS-HBC.

($R_P = 10M\Omega$), $Z_P \gg Z_L$, and hence $V_{QSL} \gg V_{EQS-HBC}$ (Figure 7(c)). Finally, as seen from (Fig.7.7(d)), when both Z_P and Z_L are low ($Z_P \gg Z_L = 50\Omega$), $R_{body} \gg Z_L$ and $Z_{skin} \gg Z_L$, and hence the maximum drop occurs across the skin and body impedances. So, both V_{EM} and $V_{EQS-HBC}$ are very small, although $V_{QSL} \geq V_{EQS-HBC}$, since $I_{QSL} \sim I_{EQS-HBC} + I_{body}$.

The simulation results of our proposed EQS-HBC circuit model (Fig.7.7(e-h)) closely matches the actual measurement results in terms of the voltage swing for both the received EQS-HBC signal and the EQS-HBC QS leakage with varying load conditions. This not only shows that the proposed EQS-HBC circuit model is accurate, but also confirms that the QS leakage signature is inverted. The inversion of QS leakage signature is due to the fact that the probe directly couples with the ground terminal (N) of the transmitter device, which is picked up by an attacker.

7.4.7 Countermeasure against the EQS-HBC transmitter QS Leakage & Experimental Validation

The goal is to develop a countermeasure against the EQS-HBC transmitter leakage. From the experiments and the developed circuit theoretic models, it is confirmed that the

EQS-HBC transmitter leaks only when aided by the human body. Now, we demonstrate a technique to reduce this QS leakage.

As shown in Fig.7.8(a), a high resistance (R_{SN}) is inserted in series to de-couple the shield (Sh) from the ground terminal (N) of the transmitter. As most of the voltage signal is dropped across R_{SN}, V_{QSL} reduces significantly, as seen from Fig.7.8(b). However, the EQS-HBC received voltage ($V_{EQS-HBC}$) also reduces as the current in the return path gets reduced.

When the resistance R_{SN}=0 (without the countermeasure - Fig.7.6(a)), with both QS and EQS-HBC probes connected at the shield and the fingers of the device hand respectively, the received EQS-HBC voltage ($V_{EQS-HBC}$) is 300 mV, while the signal from the source of the QS leakage (probe directly connected to the transmitter shield: d = 0) is $V_{QSL} \sim 3V$ (Fig.7.8(b)). With the probe disconnected, the EQS-HBC received signal level is $\sim 30mV$, which can be reliably decoded in the EQS-HBC receiver device. When the probe is not in direct contact to the transmitter shield but is in close proximity ($d = 0^+$) the amount of QS leakage signal received is $\sim 170mV$. As the series resistance (R_{SN}) is inserted and increased, both V_{QSL} and $V_{EQS-HBC}$ gets reduced, and beyond $R_{SN} = 3M\Omega$, $V_{EQS-HBC}$ goes below 10 mV, and can no longer be detected by present EQS-HBC receiver.

Hence, connecting the entire shield with a high resistance to ground is not a judicious solution as it can impede EQS-HBC. Also, having the shield fully connected to the ground potential of the transmitter leaks QS signals, which may be intercepted by an almost-touching adversary.

The above observations infer that there exists an optimization between the size of the shield plane that can be directly connected to the transmitter ground, and rest of the shield plane connected to the ground plane through the high resistance R_{SN}. Depending on the application and device form factor, the optimum shield sizes, pattern and ground plane size can be customized based on the fundamental understanding and models developed in this work.

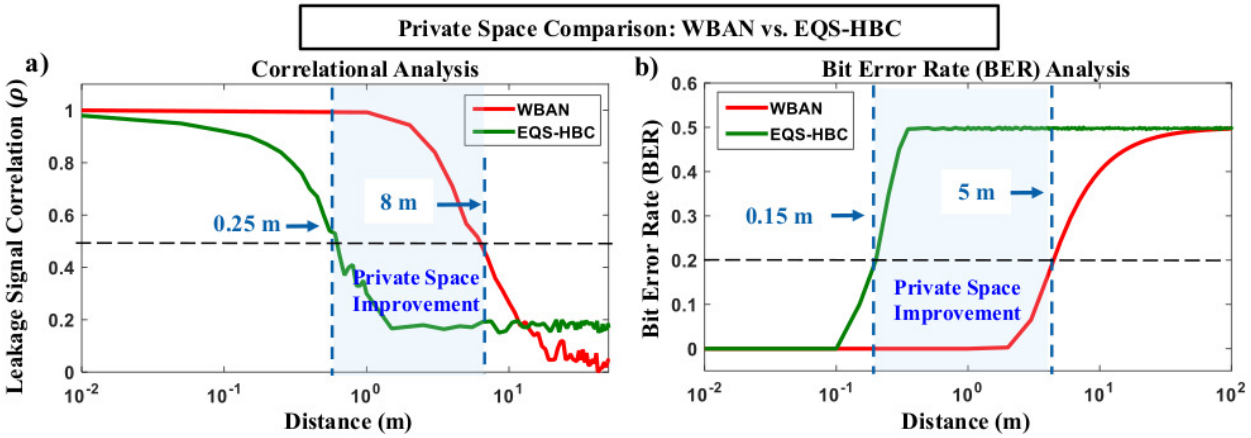


Figure 7.9. Private Space Comparison for EQS-HBC vs. WBAN. Correlational and BER analysis of the leaked "side-channel" EM signals to determine the range till which an attacker can intercept the transmitted data. EQS-HBC provides $> 30\times$ improvement in private space over traditional WBANs. The distance is defined from the device hand. Note that the EQS-HBC transmit device signal amplitude is 3.3 V, while the WBAN signal transmission power is -40 dBm. For WBAN, a 2.4 GHz carrier frequency with 1 MHz data rate, and a 6 dB noise figure for the wireless receiver was considered for the analysis. Note that increase in transmit power ($> -40dBm$) in the case of WBAN or considering more idealistic loss exponent (d^2) will only increase the range ($> 5m$) for WBAN signals in which it can be snooped by an attacker, making an even stronger case for EQS-HBC advantage over WBAN in terms of physical security/privacy.

7.5 Privacy Space Comparison: EQS-HBC vs. WBAN

To substantiate the security benefits of EQS-HBC over the traditional WBAN, a private-space comparison is necessary. In a WBAN, signals are radiated wirelessly through free space, and even considering a very low transmission power of -40 dBm and the free space path loss (FSPL) varying with the cube of the transmit distance (d^3), a known data sequence can be detected using auto-correlation based techniques over a distance of 8 m, as shown in Fig. 7.9(a). In the case of EQS-HBC, the QS leakage for a known data sequence can be detected up to a distance of 0.25 m, which is practically very close to physical contact with the person. Although auto-correlation serves for a fair comparison, it is an exaggerated attack model, since it only holds good for a known bit sequence.

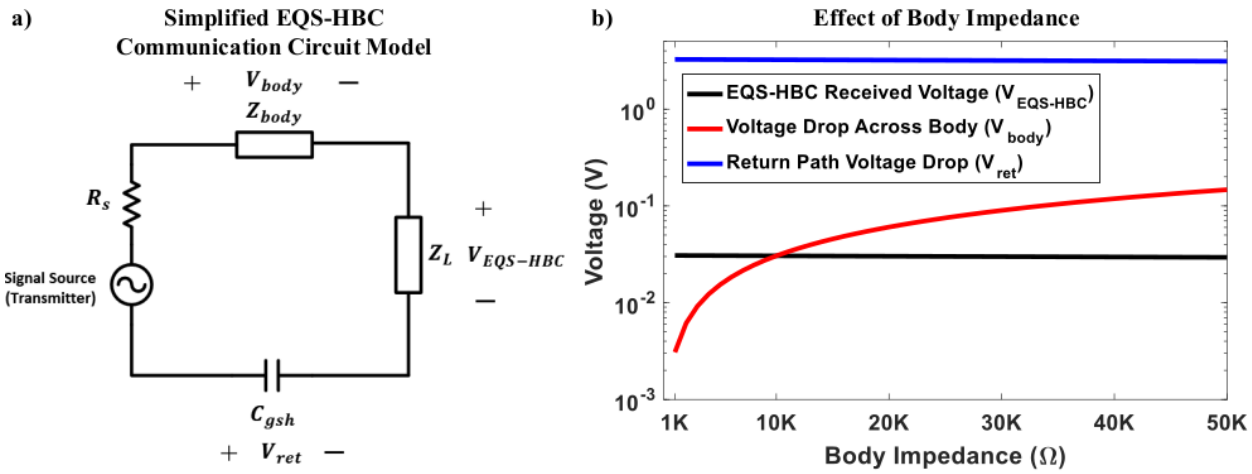


Figure 7.10. (a) Simplified EQS-HBC Circuit model with the forward path components lumped into a single impedance. (b) Effect of body impedance on the EQS-HBC received voltage ($V_{EQS-HBC}$), voltage drop across the human body (V_{body}), and the return path voltage drop (across C_{gsh}) for a 3.3V transmitted voltage at 1 MHz. Variation of body impedance in the range of tens of Kiloohms does not affect the EQS-HBC received voltage since the load impedance (Z_L) and the return path impedance values are orders of magnitude larger than the forward path body impedance.

Bit Error Rate (BER) analysis (Fig. 7.9(b)) is a more practical approach that works for any pseudo-random bit sequence (PRBS). For a BER of < 0.2 (at most 1 out of 5 bits are incorrect for a long sequence), WBAN signals can be detected up to 5 m in space, whereas EQS-HBC signals can be detected only up to 0.15 m, enabling $> 30\times$ improvement in private space compared to WBAN. Hence, EQS-HBC provides inherent data privacy and can enable steganographic covert communication.

7.6 Discussion

Different skin conditions/thickness as well as the physiologic states such as highly edematous or dehydrated cachectic conditions can alter the body fluidic conditions. This would change the skin and tissue impedances (R_{skin}, C_{skin}, R_{body}) that are considered in the lumped bio-physical model of EQS-HBC (Fig. 7.6(b)).

The simplified EQS-HBC circuit model with the forward path components lumped into a single impedance is shown in Fig. 7.10(a). The closed loop in case of capacitively-coupled

electro-quasistatic human body communication (EQS-HBC) is formed by the return path capacitance (C_{gsh}) between the transmitter and receiver which is in the order of hundreds of femtofarads (estimation of the return path capacitance (C_{gsh}) is performed by connecting several known value capacitances (C_{expt}) between the identical transmitter and the receiver device ground and measuring the loss for each case). Hence the impedance provided by the return path capacitance is $> 1M\Omega$ for the frequency range of $< 1MHz$. However, all the forward path body components (between the transmitter and receiver) considered in the human body model has impedance values in the order of tens of $K\Omega$ [160], [161]. Since the return path capacitance has the highest impedance, the closed loop current is primarily determined by its value and is very weakly dependent on the forward path components. Also, the received voltage is measured across the load, which is primarily capacitive (C_L) due to the very high resistive component (R_L) of the receiver input impedance. So, the measured channel loss is primarily determined by the capacitive division between the load capacitance and the return path capacitance ($\frac{Z_L}{Z_{body}+Z_{C_{gsh}}+Z_L} \approx \frac{C_{gsh}}{C_{gsh}+C_L}, since Z_{body} \ll Z_{C_{gsh}} + Z_L$).

Thus, the communication path loss for EQS-HBC is almost independent of the body impedance, as seen from Fig. 7.10(b) (black curve – received signal $\sim 30mV$ is consistent with the received signal as shown in Fig. 7.3: green curve). Hence, the received EQS-HBC signal across the body will have the same value irrespective of the body conditions (edematous or cachectic) or different skin thickness, as long as it is terminated by a high impedance load.

7.7 Conclusions

To conclude, this work for the first time, analyzes the security of electro-quasistatic human body communication (EQS-HBC) using the human body as the communication channel. The source of the information leakage is the EQS-HBC transmitter device aided by the human body that provides a low resistance closed path through the earth ground. The Faraday cage, which acts as the shield for the transmitter, reduces the effect of the QS leakage from the standalone transmitter, but it serves as a ground plane to increase both the EQS-HBC received potential as well as the information leakage. A fascinating observation was that

although the capacitive EQS-HBC signals from the device hand suffer low loss and maintain similar amplitude at the receiving end, the QS leakage is negligible even very close to the receiving free hand, proving that the human body does not leak information. The proposed circuit theoretic model for EQS-HBC corroborates all the measurement results and allows for countermeasures to minimize the QS leakage while maximizing the EQS-HBC received potential. De-coupling the shield and the ground of the transmitter using a high resistance reveals that both the QS leakage as well as the EQS-HBC received potential gets reduced. Hence, there exists an optimization between the area of the shield plane that connects directly to the transmitter ground potential, and rest of the shield connected to the ground plane through the high resistance R_{SN}. Finally, we show that WBAN signals can be intercepted even at a distance of 5 m, while EQS-HBC signals can only be detected up to 0.15 m, which is practically in physical contact with the person. Thus, EQS-HBC offers $> 30\times$ improvement in private space compared to the traditional WBAN, thereby enabling a covert body area network.

7.8 Methods

7.8.1 Experimental Set-up for the EQS-HBC and QS Leakage Measurement

The transmitter device for EQS-HBC was developed using off-the-shelf components (Fig. 7.11(c, d)) and the signal was coupled to the human body (skin) using an interfacing band consisting of copper electrodes ($0.02m \times 0.02m$) as discussed earlier in the article. In order to emulate a wearable device, the transmitter is battery-powered. The communication module is implemented using a Texas Instruments LaunchPad evaluation kit (TM4C123G) consisting of an ARM Cortex M4 based microcontroller (TM4C123GH6PM), which transmits the data. A rechargeable Lithium ion battery is used as power supply. The transmitter device was shielded using a copper-coated box to eliminate the QS leakage due to the standalone transmitter. Fig. 7.11(a, b) demonstrates the basic leakage measurement set-up with the wearable EQS-HBC device using an antenna and the oscilloscope (time-domain) or spectrum analyzer (frequency domain). The QS leakage from the device arm is measured with the device arm extended towards the antenna, and the distance (d) is measured between the

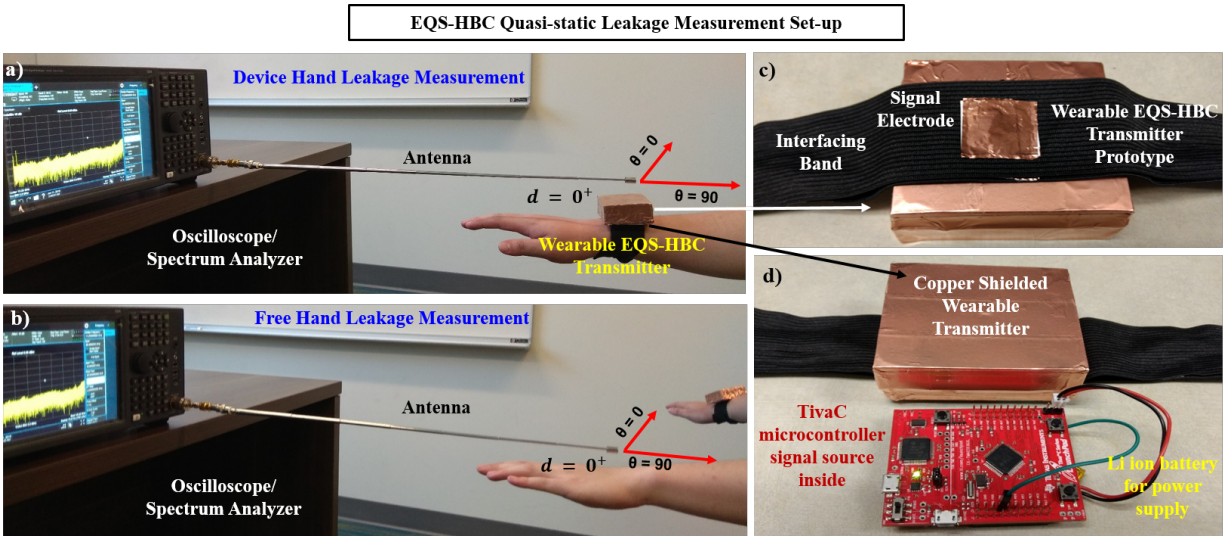


Figure 7.11. Quasi-static Leakage (QSL) Measurement Set-up with the wearable EQS-HBC device, using an antenna and an oscilloscope. (a) Leakage from the device hand is measured with the device arm extended towards the antenna tip and moving away from/towards the antenna. Distance (d) is measured between the antenna and the device. This figure shows measurement for $d = 0^+$ (very close to the antenna, but not touching it). Gradually, the device hand is moved further away from the antenna in two directions ($\theta = 0, 90$) and the leakage signal is measured and sent to the PC for further BER/correlational analysis. (b) Similarly, leakage from the free hand is measured with distance (d) between the free hand tip and the antenna tip. This figure shows measurement for $d = 0^+$. Note that during the free hand leakage measurement, it is away from the body as well as the device hand to ensure that the leakage from the EQS-HBC device arm do not affect the free arm leakage measurements. (c) The shielded wearable EQS-HBC transmit device is shown. It consists of the interfacing band with the copper electrode (signal electrode) which couples the transmitted signal into the body. (d) Inside the shield is the ARM Cortex M4 based microcontroller (TivaC) which transmits the data.

antenna tip and the body-worn EQS-HBC device. Similarly, for the free hand, leakage is measured with distance as the free hand is extended and moved away/towards the antenna. The extension of the free arm towards the antenna during the leakage measurements ensure that any QS leakage from the device arm do not affect the measurements.

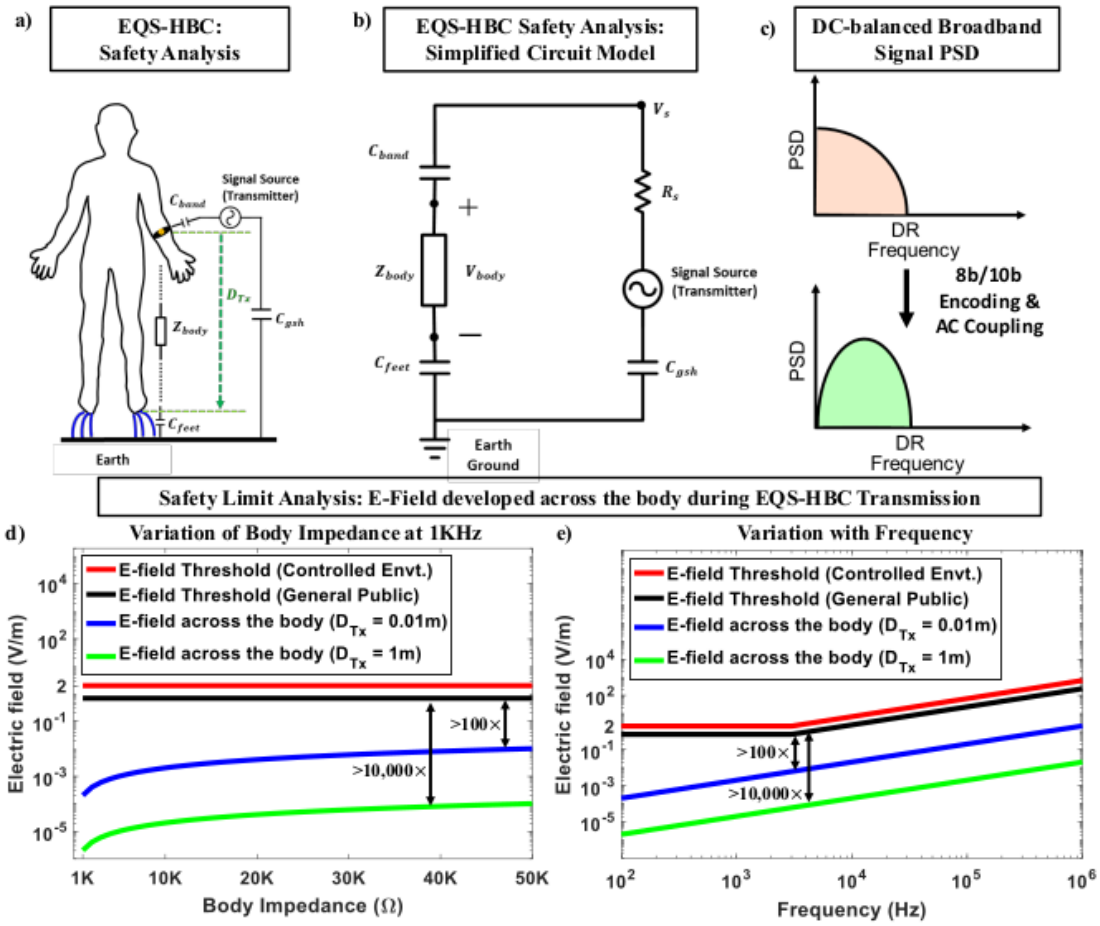


Figure 7.12. (a, b) EQS-HBC signal excitation simplified circuit model with the forward path components lumped to a single impedance (Z_{body}). C_{band} refers to the series coupling capacitor at the output of the transmit device along with the interfacing copper electrode band capacitance formed between the transmit device and the human body, D_{Tx} denotes the on-body distance for signal transmission from the transmit device to the feet, which would give the voltage drop across the body (V_{body}). (c) Power Spectral Density (PSD) of a broadband transmitted signal occupying the complete bandwidth from DC up to the data rate (DR). Bottom: PSD of the broadband transmitted signal after dc-balancing with 8b/10b encoding scheme. (d) Electric field developed across the body at a low frequency of 1 KHz is orders of magnitude lower than the IEEE defined threshold of 2.1 V/m (controlled environment) or 0.701 V/m (general public) [172], [173], for varying forward path body impedances (emulating different skin conditions) in the range of few Kiloohms. (e) Even with varying frequencies, the developed E-field across the body is orders of magnitude lower than the IEEE defined thresholds [172], [173], at those frequencies.

7.8.2 Safety Limit Compliance in EQS-HBC

The circuit model of the EQS-HBC during the signal transmission is shown in Fig. 7.12(a, b). For safety analysis, only the transmitter is considered as the current distribution is mostly independent of the receiver (high impedance termination). The transmitted signal needs to be biphasic to avoid any harmful electrochemical reactions [174]. For EQS-HBC, the PRBS data sequence is a series of 0's and 1's. A series coupling capacitor at the output of the transmit device, along with the interfacing copper electrode band capacitance (C_{band}) formed between the transmit device and the human body provides the AC coupling, as shown in Fig. 7.12(a). Hence, the signals are converted to AC, and contains both positive and negative phases. The sequence is dc-balanced with the capacitive coupling and 8b/10b encoding scheme, and hence the PSD of the transmitted broadband signal for EQS-HBC (after dc balancing) gets modified as shown in Fig. 7.12(c). Fig. 7.12(b) shows the simplified circuit model of the EQS-HBC transmission with the forward path components lumped into a single impedance (Z_{body}). R_s denotes the series resistance of the signal source, C_{feet} represents the capacitance between the feet and the earth's ground, and C_{gsh} is the return path capacitance between the shielded transmitter and the earth's ground. D_{Tx} is the on-body distance for signal transmission from the transmit device to the feet, which gives the voltage drop across the body (V_{body}).

The safety limit analysis for the developed electric field across the human body is shown in Fig. 7.12(c, d). The E-field thresholds in compliance with the IEEE standards [172], [173], are also shown in Fig. 7.12(c, d). Fig. 7.12(c) shows variation of the E-field with the body impedance (emulating the different skin conditions, across different persons, or even time of the day), and Fig. 7.12(d) shows the E-field for varying frequencies for $Z_{body} = 10K\Omega$ (typical body impedance is in the range of tens of kilo ohms [160], [161]). It can be clearly seen that the E-field developed across the body is orders of magnitude lower than the threshold even for $D_{Tx} = 0.01m$ (that is, when the EQS-HBC transmit device is very close to the feet) for different frequencies as well as for varying forward path body impedances.

Also, the amount of current which is perceptible to a human is 1mA ac [160], [175]. The ventricular fibrillation threshold is 100 mA and a current of 2 A can cause a cardiac standstill

and internal organ damage [160], [175]. However, for the case of EQS-HBC, the amount of current passing through the body is in the order of few microamps (μA), since the voltage drop across the body is below 10 mV (as shown in Fig. 7.10 – red curve) and the body resistance is in the order of tens of kilo ohms. Hence, the current through the body during EQS-HBC is at least three orders of magnitude lower than the perceptible threshold.

The experimental protocols involving human subjects have been approved by the Purdue Institutional Review Board (IRB Protocol #1610018370) and also approved by the Air Force Office of Scientific Research (AFOSR), Department of Defense (DoD) through a 2^nd level review. All guidelines and regulations, as given by the Purdue IRB, and AFOSR were followed during the experiments. The authors also confirm that informed consent was obtained from all participants for the experiments.

Multiple follow-up works [176], [177], [178], [179], [180], [168], [181], [182], [183], [184], [185] motivated by the development of EQS-HBC have been proposed recently.

8. SUMMARY & FUTURE DIRECTIONS

In this thesis, we have investigated both secure computation as well as secure communication. In secure computation, we developed advanced side-channel attacks and proposed low-overhead generic countermeasures to counter such EM/power SCA attacks on crypto devices through a ground-up root-cause analysis. Specifically, we proposed the first cross-device deep-learning based SCA attack on embedded devices [34].

A white-box modeling approach was presented [37], which showed that the higher level metal layers are the main cause of the EM leakage and hence we proposed the STELLAR technique to encapsulate the crypto core locally within the lower-level metal layers using a current-domain signature attenuation (CDSA) hardware [40], [43], [42]. The CDSA hardware fabricated in TSMC 65nm process showed a $> 350\times$ signature attenuation on the AES-256 encryption traces, achieving $> 1B$ MTD, which is the highest SCA security reported till date ($> 100\times$ compared to the previous works) with comparable overheads. This is also a generic technique, which is agnostic of the crypto algorithm and does not have any performance degradation. The CDSA-AES256 is also evaluated against deep-learning based SCA attacks, and showed that the neural network could not be trained even with $10M$ traces [47].

Next, we showed the development of the first pre-Si EM SCA evaluation framework combining Virtuoso and HFSS, and proposed a modified standard library cell layout for minimizing the EM SCA leakage [39].

Finally, we pioneered and analyzed the physical security of electro-quasistatic human body communication (EQS-HBC) and showed a $> 30\times$ improvement in the private space compared to the traditional WBANs [48]. Since this work, multiple follow-up works on implementing EQS-HBC on-chip have been demonstrated recently [183], [51], [50].

Many of the works presented in this thesis have been already adopted in the industry to protect their IPs against these growing EM/power SCA attacks. Several follow-up works [117], [35], [36], [186], [187], [188], [189], [190], [191], [115], [192], [193], [194], [195], [196] have been published recently as well. [196], [188], [189], [195] have mainly focused on making the countermeasure more digital-friendly and scalable across different process nodes. [115] shows a physics-based analysis of the effect of power grid routing structures on the EM

leakage. [117] proposed the SCNIFFER framework for making the EM SCA attack more automated, efficient, and faster. [35], [36] advanced the proposed `X-DeepSCA` attack for more number of devices as well as extending towards cross-device EM ML SCA. [186] utilized the STELLAR framework and incorporated a blinking technique to turn on the countermeasure only at the points of high leakage during the crypto operations, thereby reducing the power overhead significantly. [192], [193] proposed an approaching EM probe detection technique to augment with our proposed countermeasure, so that the countermeasure is pro-actively turned on whenever an imminent attack is detected.

In future, with the growth of more internet-connected devices, we will continue to see the rising trend in power and EM SCA analysis, specifically for newer algorithms like post-quantum cryptography and homomorphic encryption. Also, remote software-based SCA attacks will continue to increase and hence deploying low-cost, scalable, and generic mitigations at the pre-silicon level becomes extremely critical for all IoT and embedded devices.

REFERENCES

[1] J. M. Rabaey, "A brand new wireless day," in *2008 Asia and South Pacific Design Automation Conference*, ISSN: 2153-697X, Mar. 2008, pp. 1–1. DOI: 10.1109/ASPDAC.2008.4483940.

[2] M. G. Institute, "The internet of things: Mapping the value beyond the hype," McKinsey Global Institute, Tech. Rep., Jun. 2015.

[3] S. Sen, "Internet of Things: Sensor Nodes," 2020. DOI: https://nanohub.org/resources/33738.

[4] J. Yang, B. Chatterjee, M. Thorsell, M. Kowalewski, B. Edward, D. Peroulis, and S. Sen, "Instinctual Interference-Adaptive Low-Power Receiver With Combined Feedforward and Feedback Control," *IEEE Microwave and Wireless Components Letters*, vol. 31, no. 6, pp. 771–774, Jun. 2021, Conference Name: IEEE Microwave and Wireless Components Letters, ISSN: 1558-1764. DOI: 10.1109/LMWC.2021.3067912.

[5] K. Gaurav Kumar, B. Chatterjee, and S. Sen, "A 16 pJ/bit 0.1-15Mbps Compressive Sensing IC with on-chip DWT Sparsifier for Audio Signals," in *2021 IEEE Custom Integrated Circuits Conference (CICC)*, ISSN: 2152-3630, Apr. 2021, pp. 1–2. DOI: 10.1109/CICC51472.2021.9431569.

[6] B. Chatterjee and S. Sen, "Energy-Efficient Deep Neural Networks with Mixed-Signal Neurons and Dense-Local and Sparse-Global Connectivity," in *Proceedings of the 26th Asia and South Pacific Design Automation Conference*, ser. ASPDAC '21, New York, NY, USA: Association for Computing Machinery, Jan. 2021, pp. 297–304, ISBN: 978-1-4503-7999-1. DOI: 10.1145/3394885.3431614. [Online]. Available: https://doi.org/10.1145/3394885.3431614.

[7] B. Chatterjee, P. Panda, S. Maity, A. Biswas, K. Roy, and S. Sen, "Exploiting Inherent Error Resiliency of Deep Neural Networks to Achieve Extreme Energy Efficiency Through Mixed-Signal Neurons," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 6, pp. 1365–1377, Jun. 2019, Conference Name: IEEE Transactions on Very Large Scale Integration (VLSI) Systems, ISSN: 1557-9999. DOI: 10.1109/TVLSI.2019.2896611.

[8] S. Sen, "Invited: Context-aware energy-efficient communication for IoT sensor nodes," in *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, Jun. 2016, pp. 1–6. DOI: 10.1145/2897937.2905005.

[9] B. Chatterjee, N. Cao, A. Raychowdhury, and S. Sen, "Context-Aware Intelligence in Resource-Constrained IoT Nodes: Opportunities and Challenges," *IEEE Design Test*, vol. 36, no. 2, pp. 7–40, Apr. 2019, Conference Name: IEEE Design Test, ISSN: 2168-2364. DOI: 10.1109/MDAT.2019.2899334.

[10] B. Chatterjee, D.-H. Seo, S. Chakraborty, S. Avlani, X. Jiang, H. Zhang, M. Abdallah, N. Raghunathan, C. Mousoulis, A. Shakouri, S. Bagchi, D. Peroulis, and S. Sen, "Context-Aware Collaborative-Intelligence with Spatio-Temporal In-Sensor-Analytics in a Large-Area IoT Testbed," *arXiv:2005.13003 [cs, eess]*, Nov. 2020, arXiv: 2005.13003. [Online]. Available: http://arxiv.org/abs/2005.13003.

[11] N. Cao, S. B. Nasir, S. Sen, and A. Raychowdhury, "In-sensor analytics and energy-aware self-optimization in a wireless sensor node," in *2017 IEEE MTT-S International Microwave Symposium (IMS)*, Jun. 2017, pp. 200–203. DOI: 10.1109/MWSYM.2017.8059047.

[12] S. Avlani, D. Seo, B. Chatterjee, and S. Sen, "EICO: Energy-Harvesting Long-Range Environmental Sensor Nodes with Energy-Information Dynamic Co-Optimization," *arXiv:2107.07072 [cs, eess]*, Jul. 2021, arXiv: 2107.07072. [Online]. Available: http://arxiv.org/abs/2107.07072.

[13] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*, ISSN: 2375-1207, May 2017, pp. 195–212. DOI: 10.1109/SP.2017.14.

[14] S. Sen, S. Maity, and D. Das, "The body is the network: To safeguard sensitive data, turn flesh and tissue into a secure wireless channel," *IEEE Spectrum*, vol. 57, no. 12, pp. 44–49, Dec. 2020, Conference Name: IEEE Spectrum, ISSN: 1939-9340. DOI: 10.1109/MSPEC.2020.9271808.

[15] TEDx Talks, *How your body can play an integral role in wearable security | Shreyas Sen | TEDxIndianapolis*. [Online]. Available: https://www.youtube.com/watch?v=6NKGX-sinOA&list=PLV45P77Yo8yepm4yVPNENy98hEOw2juel&ab_channel=TEDxTalks.

[16] M. K. Kim, C. Kantarcigil, B. Kim, R. K. Baruah, S. Maity, Y. Park, K. Kim, S. Lee, J. B. Malandraki, S. Avlani, A. Smith, S. Sen, M. A. Alam, G. Malandraki, and C. H. Lee, "Flexible submental sensor patch with remote monitoring controls for management of oropharyngeal swallowing disorders," en, *Science Advances*, vol. 5, no. 12, eaay3210, Dec. 2019, Publisher: American Association for the Advancement of Science Section: Research Article, ISSN: 2375-2548. DOI: 10.1126/sciadv.aay3210. [Online]. Available: https://advances.sciencemag.org/content/5/12/eaay3210.

[17] M. Parsa, P. Panda, S. Sen, and K. Roy, "Staged Inference using Conditional Deep Learning for energy efficient real-time smart diagnosis," eng, *Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference*, vol. 2017, pp. 78–81, Jul. 2017, ISSN: 2694-0604. DOI: 10.1109/EMBC.2017.8036767.

[18] *Can "Internet-of-Body" Thwart Cyber Attacks on Implanted Medical Devices? - IEEE Spectrum*, en. [Online]. Available: https://spectrum.ieee.org/the-human-os/biomedical/devices/thwart-cyber-attacks-on-implanted-medical-devices.

[19] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, Feb. 2019, Conference Name: IEEE Internet of Things Journal, ISSN: 2327-4662. DOI: 10.1109/JIOT.2018.2849324.

[20] B. Chatterjee, D. Das, and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Apr. 2018, pp. 205–208. DOI: 10.1109/HST.2018.8383916.

[21] M. F. Bari, B. Chatteijee, and S. Sen, "DIRAC: Dynamic-IRregulAr Clustering Algorithm with Incremental Learning for RF-Based Trust Augmentation in IoT Device Authentication," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, ISSN: 2158-1525, May 2021, pp. 1–5. DOI: 10.1109/ISCAS51556.2021.9401403.

[22] R. Callan, A. Zajic, and M. Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events," in *2014 47th Annual IEEE/ACM International Symposium on Microarchitecture*, ISSN: 2379-3155, Dec. 2014, pp. 242–254. DOI: 10.1109/MICRO.2014.39.

[23] N. Sehatbakhsh, A. Nazari, A. Zajic, and M. Prvulovic, "Spectral profiling: Observer-effect-free profiling by monitoring EM emanations," in *2016 49th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, Oct. 2016, pp. 1–11. DOI: 10.1109/MICRO.2016.7783762.

[24] L. N. Nguyen, B. B. Yilmaz, M. Prvulovic, and A. Zajic, "A Novel Golden-Chip-Free Clustering Technique Using Backscattering Side Channel for Hardware Trojan Detection," English, IEEE Computer Society, Dec. 2020, pp. 1–12, ISBN: 978-1-72817-405-1. DOI: 10.1109/HOST45689.2020.9300127. [Online]. Available: https://www.computer.org/csdl/proceedings-article/host/2020/09300127/1pQJ1yRn8jK.

[25] B. Krebs, *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, en-US, Library Catalog: krebsonsecurity.com. [Online]. Available: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

[26] V. LOMNE and T. ROCHE, "A Side Journey to Titan," Tech. Rep. 028, 2021. [Online]. Available: https://eprint.iacr.org/2021/028.

[27] O. Lisovets, D. Knichel, T. Moos, and A. Moradi, "Let's Take it Offline: Boosting Brute-Force Attacks on iPhone's User Authentication through SCA," Tech. Rep. 460, 2021. [Online]. Available: https://eprint.iacr.org/2021/460.

[28] M. Lipp, A. Kogler, D. Oswald, M. Schwarz, C. Easdon, C. Canella, and D. Gruss, "PLATYPUS: Software-Based Power Side-Channel Attacks on x86," English, ISSN: 2375-1207, IEEE Computer Society, pp. 355–371, ISBN: 978-1-72818-934-5. DOI: 10.1109/SP40001.2021.00063. [Online]. Available: https://www.computer.org/csdl/proceedings-article/sp/2021/893400b080/1t0x8XZU9ry.

[29] C. Ramesh, S. B. Patil, S. N. Dhanuskodi, G. Provelengios, S. Pillement, D. Holcomb, and R. Tessier, "FPGA Side Channel Attacks without Physical Access," in *2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, ISSN: 2576-2621, Apr. 2018, pp. 45–52. DOI: 10.1109/FCCM.2018.00016.

[30] J. Krautter, D. R. E. Gnad, and M. B. Tahoori, "Mitigating Electrical-level Attacks towards Secure Multi-Tenant FPGAs in the Cloud," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 12, no. 3, 12:1–12:26, Aug. 2019, ISSN: 1936-7406. DOI: 10.1145/3328222. [Online]. Available: https://doi.org/10.1145/3328222.

[31] R. Elnaggar, R. Karri, and K. Chakrabarty, "Multi-Tenant FPGA-based Reconfigurable Systems: Attacks and Defenses," in *2019 Design, Automation Test in Europe Conference Exhibition (DATE)*, ISSN: 1558-1101, Mar. 2019, pp. 7–12. DOI: 10.23919/DATE.2019.8714904.

[32] D. Genkin et al., "Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation," en, in *CHES 2015*, Springer, Berlin, Heidelberg, Sep. 2015, pp. 207–228, ISBN: 978-3-662-48323-7 978-3-662-48324-4. DOI: 10.1007/978-3-662-48324-4_11.

[33] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18, Toronto, Canada: Association for Computing Machinery, Jan. 2018, pp. 163–177, ISBN: 978-1-4503-5693-0. DOI: 10.1145/3243734.3243802. [Online]. Available: https://doi.org/10.1145/3243734.3243802.

[34] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, and S. Sen, "X-DeepSCA: Cross-Device Deep Learning Side Channel Attack," in *2019 56th ACM/IEEE Design Automation Conference (DAC)*, ISSN: 0738-100X, Jun. 2019, pp. 1–6.

[35] A. Golder, D. Das, J. Danial, S. Ghosh, S. Sen, and A. Raychowdhury, "Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2720–2733, Dec. 2019, ISSN: 1557-9999. DOI: 10.1109/TVLSI.2019.2926324.

[36] J. Danial, D. Das, A. Golder, S. Ghosh, A. Raychowdhury, and S. Sen, "Em-x-dl: Efficient cross-device deep learning side-channel attack with noisy em signatures," *ACM Journal on Emerging Technologies in Computing Systems*, 2021.

[37] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis," in *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2019, pp. 11–20. DOI: 10.1109/HST.2019.8740839.

[38] D. Das, M. Nath, S. Ghosh, and S. Sen, "killing em side-channel leakage at its source," in *2020 IEEE MWSCAS*, ISSN: 1558-3899, Aug. 2020, pp. 1108–1111. DOI: 10.1109/MWSCAS48704.2020.9184657.

[39] D. Das, M. Nath, B. Chatterjee, R. Kumar, X. Liu, H. Krishnamurthy, M. Sastry, S. Mathew, S. Ghosh, and S. Sen, "Em sca white-box analysis based reduced leakage cell design and pre-silicon evaluation," *under review*, 2021.

[40] D. Das et al., "27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation," in *2020 IEEE International Solid-State Circuits Conference - (ISSCC)*, ISSN: 2376-8606, Feb. 2020, pp. 424–426. DOI: 10.1109/ISSCC19947.2020.9062997.

[41] D. D. et al., "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *2017 IEEE HOST*, May 2017, pp. 62–67.

[42] D. D. et al., "ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity," *IEEE TCAS-I*, pp. 1–12, 2018, ISSN: 1549-8328.

[43] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D.-H. Seo, M. Chang, A. L. Varna, H. K. Krishnamurthy, S. Mathew, S. Ghosh, A. Raychowdhury, and S. Sen, "EM and Power SCA-Resilient AES-256 Through >350x Current-Domain Signature Attenuation and Local Lower Metal Routing," *IEEE Journal of Solid-State Circuits*, pp. 1–1, 2020, Conference Name: IEEE Journal of Solid-State Circuits, ISSN: 1558-173X. DOI: 10.1109/JSSC.2020.3032975.

[44] D. Das and S. Sen, "Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach," en, *Cryptography*, vol. 4, no. 4, p. 30, Dec. 2020, Number: 4 Publisher: Multidisciplinary Digital Publishing Institute. DOI: 10.3390/cryptography4040030. [Online]. Available: https://www.mdpi.com/2410-387X/4/4/30.

[45] D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "EM/Power Side-Channel Attack: White-Box Modeling Signature Attenuation Countermeasures," *IEEE Design Test*, pp. 1–1, 2021, Conference Name: IEEE Design Test, ISSN: 2168-2364. DOI: 10.1109/MDAT.2021.3065189.

[46] D. Das, B. Chatterjee, and S. Sen, "Security of Analog, Mixed-Signal, and RF Devices," en, in *Emerging Topics in Hardware Security*, M. Tehranipoor, Ed., Cham: Springer International Publishing, 2021, pp. 391–418, ISBN: 978-3-030-64448-2. DOI: 10.1007/978-3-030-64448-2_15. [Online]. Available: https://doi.org/10.1007/978-3-030-64448-2_15.

[47] D. Das et al., "Deep Learning Side-Channel Attack Resilient AES-256 using Current Domain Signature Attenuation in 65nm CMOS," in *IEEE CICC*, 2020. DOI: 10.1109/CICC48029.2020.9075889.

[48] D. Das et al., "Enabling Covert Body Area Network using Electro-Quasistatic Human Body Communication," en, *Scientific Reports*, vol. 9, no. 1, 2019, ISSN: 2045-2322. DOI: 10.1038/s41598-018-38303-x. [Online]. Available: https://www.nature.com/articles/s41598-018-38303-x.

[49] S. Maity, M. He, M. Nath, D. Das, B. Chatterjee, and S. Sen, "BioPhysical Modeling, Characterization and Optimization of Electro-Quasistatic Human Body Communication," *arXiv:1805.05200 [cs]*, May 2018, arXiv: 1805.05200. [Online]. Available: http://arxiv.org/abs/1805.05200.

[50] N. Modak, D. Das, M. Nath, B. Chatterjee, K. Gaurav Kumar, S. Maity, and S. Sen, "A 65nm Resonant Electro-Quasistatic 5-240uW Human Whole-Body Powering and 2.19uW Communication SoC with Automatic Maximum Resonant Power Tracking," in *2021 IEEE Custom Integrated Circuits Conference (CICC)*, ISSN: 2152-3630, Apr. 2021, pp. 1–2. DOI: 10.1109/CICC51472.2021.9431456.

[51] S. Maity, N. Modak, D. Yang, M. Nath, S. Avlani, D. Das, J. Danial, P. Mehrotra, and S. Sen, "Sub- WRComm: 415-nW 1–10-kb/s Physically and Mathematically Secure Electro-Quasi-Static HBC Node for Authentication and Medical Applications," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 3, pp. 788–802, Mar. 2021, Conference Name: IEEE Journal of Solid-State Circuits, ISSN: 1558-173X. DOI: 10.1109/JSSC.2020.3041874.

[52] S. Maity, D. Yang, S. S. Redford, D. Das, B. Chatterjee, and S. Sen, "*BodyWire-HCI*: Enabling New Interaction Modalities by Communicating Strictly During Touch Using Electro-Quasistatic Human Body Communication," *ACM Transactions on Computer-Human Interaction*, vol. 27, no. 6, 39:1–39:25, Nov. 2020, ISSN: 1073-0516. DOI: 10.1145/3406238. [Online]. Available: https://doi.org/10.1145/3406238.

[53] S. Maity, D. Das, and S. Sen, "Adaptive interference rejection in Human Body Communication using variable duty cycle integrating DDR receiver," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*, Mar. 2017, pp. 1763–1768. DOI: 10.23919/DATE.2017.7927278.

[54] S. Maity, D. Das, and S. Sen, "Wearable health monitoring using capacitive voltage-mode Human Body Communication," in *2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Jul. 2017, pp. 1–4. DOI: 10.1109/EMBC.2017.8036748.

[55] S. Maity, D. Das, B. Chatterjee, and S. Sen, "Characterization and Classification of Human Body Channel as a function of Excitation and Termination Modalities," *arXiv:1805.02492 [cs]*, May 2018, arXiv: 1805.02492. [Online]. Available: http://arxiv.org/abs/1805.02492.

[56] S. Maity, D. Das, X. Jiang, and S. Sen, "Secure Human-Internet using dynamic Human Body Communication," in *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, Jul. 2017, pp. 1–6. DOI: 10.1109/ISLPED.2017.8009190.

[57] D. Das, S. Maity, B. Chatterjee, and S. Sen, "In-field Remote Fingerprint Authentication using Human Body Communication and On-Hub Analytics," *arXiv:1804.10278 [cs, eess]*, Apr. 2018, arXiv: 1804.10278. [Online]. Available: http://arxiv.org/abs/1804.10278.

[58] A. Moradi, M. Kasper, and C. Paar, "Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures," en, in *Topics in Cryptology – CT-RSA 2012*, O. Dunkelman, Ed., ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2012, pp. 1–18, ISBN: 978-3-642-27954-6.

[59] T. E. et al., "On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme," en, in *CRYPTO 2008*, 2008, pp. 203–220, ISBN: 978-3-540-85174-5.

[60] D. O. et al., "Side-Channel Attacks on the Yubikey 2 One-Time Password Generator," en, in *Research in Attacks, Intrusions, and Defenses*, 2013, pp. 204–222, ISBN: 978-3-642-41284-4.

[61] S. C. et al., "Template Attacks," en, in *CHES 2003*, 2003, pp. 13–28, ISBN: 978-3-540-36400-9.

[62] D. O. et al., "Breaking Mifare DESFire MF3icd40: Power Analysis and Templates in the Real World," en, in *CHES 2011*, 2011, pp. 207–222, ISBN: 978-3-642-23951-9.

[63] C. R. et al., "Practical Template Attacks," en, in *Information Security Applications*, 2005, pp. 440–456, ISBN: 978-3-540-31815-6.

[64] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, and J. Vandewalle, "Machine learning in side-channel analysis: A first study," en, *Journal of Cryptographic Engineering*, vol. 1, no. 4, p. 293, Oct. 2011, ISSN: 2190-8516. DOI: 10.1007/s13389-011-0023-x. [Online]. Available: https://doi.org/10.1007/s13389-011-0023-x.

[65] L. L. et al., "Template attacks versus machine learning revisited and the curse of dimensionality in side-channel analysis: Extended version," en, *Journal of Cryptographic Engineering*, vol. 8, no. 4, pp. 301–313, Nov. 2018, ISSN: 2190-8516.

[66] T. Bartkewitz and K. Lemke-Rust, "Efficient Template Attacks Based on Probabilistic Multi-class Support Vector Machines," en, in *Smart Card Research and Advanced Applications*, S. Mangard, Ed., ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2013, pp. 263–276, ISBN: 978-3-642-37288-9.

[67] E. Cagli, C. Dumas, and E. Prouff, "Convolutional Neural Networks with Data Augmentation against Jitter-Based Countermeasures – Profiling Attacks without Pre-Processing –," Tech. Rep. 740, 2017. [Online]. Available: https://eprint.iacr.org/2017/740.

[68] R. G. et al., "Neural network based attack on a masked implementation of AES," in *2015 IEEE HOST*, May 2015, pp. 106–111.

[69] H. M. et al., "Breaking Cryptographic Implementations Using Deep Learning Techniques," Tech. Rep. 921, 2016.

[70] G. Perin, B. Ege, and J. van Woudenberg, "Lowering the Bar: Deep Learning for Side-Channel Analysis (White-Paper)," en, *Blackhat 2018*, p. 15, Jul. 2018. [Online]. Available: https://data.hackinn.com/ppt/BlackHat-USA-2018/us-18-perin-ege-vanwoudenberg-Lowering-the-bar-Deep-learning-for-side-channel-analysis-wp.pdf.

[71] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," en, in *Cryptographic Hardware and Embedded Systems - CHES 2004*, M. Joye and J.-J. Quisquater, Eds., ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2004, pp. 16–29, ISBN: 978-3-540-28632-5.

[72] M. A. et al., "Tensorflow: A system for large-scale machine learning," in *12th USENIX Symposium*, Savannah, GA: USENIX Association, 2016, pp. 265–283, ISBN: 978-1-931971-33-1.

[73] D. M. et al., "Improving cross-device attacks using zero-mean unit-variance normalization," en, *Journal of Cryptographic Engineering*, vol. 3, no. 2, Jun. 2013, ISSN: 2190-8516.

[74] L. L. et al., "Power Analysis Attack: An Approach Based on Machine Learning," *Int. J. Appl. Cryptol.*, vol. 3, no. 2, pp. 97–115, Jun. 2014, ISSN: 1753-0563.

[75] L. L. et al., "A Time Series Approach for Profiling Attack," en, in *Security, Privacy, and Applied Cryptography Engineering*, 2013, pp. 75–94, ISBN: 978-3-642-41224-0.

[76] L. L. et al., "A machine learning approach against a masked AES," en, *Journal of Cryptographic Engineering*, vol. 5, no. 2, pp. 123–139, Jun. 2015, ISSN: 2190-8516.

[77] E. P. et al., "Study of Deep Learning Techniques for Side-Channel Analysis and Introduction to ASCAD Database," Tech. Rep. 053, 2018.

[78] M. R. et al., "A Formal Study of Power Variability Issues and Side-Channel Attacks for Nanoscale Devices," en, in *EUROCRYPT 2011*, 2011, pp. 109–128, ISBN: 978-3-642-20465-4.

[79] M. O. C. et al., "Efficient, Portable Template Attacks," *IEEE TIFS*, vol. 13, no. 2, pp. 490–501, Feb. 2018, ISSN: 1556-6013.

[80] N. H. et al., "Empirical evaluation of multi-device profiling side-channel attacks," in *2014 IEEE Workshop on Signal Processing Systems (SiPS)*, Oct. 2014, pp. 1–6.

[81] S. I. et al., "Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift," *arXiv:1502.03167 [cs]*, Feb. 2015.

[82] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs," Tech. Rep. 129, 2016. [Online]. Available: https://eprint.iacr.org/2016/129.

[83] E. D. Mulder et al., "Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem," in *EUROCON 2005*, vol. 2, Nov. 2005, pp. 1879–1882. DOI: 10.1109/EURCON.2005.1630348.

[84] T.-H. Le et al., "A Proposition for Correlation Power Analysis Enhancement," en, in *CHES*, Oct. 2006, pp. 174–186, ISBN: 978-3-540-46559-1 978-3-540-46561-4. DOI: 10.1007/11894063_14.

[85] C. O'Flynn, "A Framework for Embedded Hardware Security Analysis," en, Jul. 2017. [Online]. Available: https://DalSpace.library.dal.ca/handle/10222/73002.

[86] S. Mangard et al., *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, en. Springer US, 2007, ISBN: 978-0-387-30857-9.

[87] T. Guneysu and A. Moradi, "Generic Side-Channel Countermeasures for Reconfigurable Devices," en, in *CHES 2011*, Sep. 2011, pp. 33–48, ISBN: 978-3-642-23950-2 978-3-642-23951-9. DOI: 10.1007/978-3-642-23951-9_3.

[88] E. Peeters et al., "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integration, the VLSI Journal*, Embedded Cryptographic Hardware, vol. 40, no. 1, pp. 52–60, Jan. 2007, ISSN: 0167-9260. DOI: 10.1016/j.vlsi.2005.12.013.

[89] C. O'Flynn and Z. (Chen, "ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research," en, in *Constructive Side-Channel Analysis and Secure Design*, E. Prouff, Ed., ser. Lecture Notes in Computer Science, Springer International Publishing, 2014, pp. 243–260, ISBN: 978-3-319-10175-0.

[90] D. Agrawal et al., "The EM Side—Channel(s)," en, in *CHES*, Aug. 2002, pp. 29–45, ISBN: 978-3-540-00409-7 978-3-540-36400-9. DOI: 10.1007/3-540-36400-5_4.

[91] T. Ordas et al., "Near-Field Mapping System to Scan in Time Domain the Magnetic Emissions of Integrated Circuits," en, Sep. 2008, pp. 229–236, ISBN: 978-3-540-95947-2 978-3-540-95948-9. DOI: 10.1007/978-3-540-95948-9_23.

[92] V. Lomne et al., "Evaluation on FPGA of Triple Rail Logic Robustness Against DPA and DEMA," ser. DATE, 2009, pp. 634–639, ISBN: 978-3-9810801-5-5.

[93] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, "Efficient simulation of EM side-channel attack resilience," in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, ISSN: 1558-2434, Nov. 2017, pp. 123–130. DOI: 10.1109/ICCAD.2017.8203769.

[94] N. Homma, Y.-i. Hayashi, N. Miura, D. Fujimoto, D. Tanaka, M. Nagata, and T. Aoki, "EM Attack Is Non-invasive? - Design Methodology and Validity Verification of EM Attack Sensor," en, in *Cryptographic Hardware and Embedded Systems – CHES 2014*, ser. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Sep. 2014, pp. 1–16, ISBN: 978-3-662-44708-6 978-3-662-44709-3. DOI: 10.1007/978-3-662-44709-3_1. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-662-44709-3_1.

[95] M. Yamaguchi et al., "Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis," in *2010 IEEE International Symposium on Electromagnetic Compatibility*, Jul. 2010, pp. 103–108. DOI: 10.1109/ISEMC.2010.5711255.

[96] O. Reparaz et al., "Consolidating Masking Schemes," en, in *CRYPTO*, ser. Lecture Notes in Computer Science, Aug. 2015, pp. 764–783, ISBN: 978-3-662-47988-9 978-3-662-47989-6. DOI: 10.1007/978-3-662-47989-6_37.

[97] S. Natarajan et al., "A 32nm logic technology featuring 2nd-generation high-k + metal-gate transistors, enhanced channel strain and 0.171 um2 SRAM cell size in a 291mb array," in *2008 IEEE International Electron Devices Meeting*, Dec. 2008, pp. 1–3. DOI: 10.1109/IEDM.2008.4796777.

[98] C. A. Balanis, *Antenna Theory: Analysis and Design*, English, 4 edition. Hoboken, NJ: Wiley, Feb. 2016, ISBN: 978-1-118-64206-1.

[99] P. Packan et al., "High performance 32nm logic technology featuring 2nd generation high-k + metal gate transistors," en, IEEE IEDM, Dec. 2009, pp. 1–4, ISBN: 978-1-4244-5639-0. DOI: 10.1109/IEDM.2009.5424253.

[100] T. D. Solutions, *Tekbox EMC Near-field Probes Manual*.

[101] A. EM Probe Manual, *RF Near Field Probe Set DC to 9ghz*.

[102] K. Tiri et al., "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proceedings of the 28th European Solid-State Circuits Conference*, Sep. 2002, pp. 403–406.

[103] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual-Rail Pre-charge Logic," en, in *Cryptographic Hardware and Embedded Systems - CHES 2006*, ser. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Oct. 2006, pp. 232–241, ISBN: 978-3-540-46559-1 978-3-540-46561-4. DOI: 10.1007/11894063_19. [Online]. Available: https://link.springer.com/chapter/10.1007/11894063_19.

[104] D. D. Hwang, K. Tiri, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "AES-Based Security Coprocessor IC in 0.18-$muhbox m$CMOS With Resistance to Differential Power Analysis Side-Channel Attacks," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006, ISSN: 0018-9200. DOI: 10.1109/JSSC.2006.870913.

[105] T. D. Cnudde et al., "Hardware Masking, Revisited," en, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 2, pp. 123–148, May 2018, ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i2.123-148.

[106] C. Tokunaga and D. Blaauw, "Securing Encryption Systems With a Switched Capacitor Current Equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010, ISSN: 0018-9200. DOI: 10.1109/JSSC.2009.2034081.

[107] A. Singh, M. Kar, A. Rajan, V. De, and S. Mukhopadhyay, "Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2016, pp. 145–148. DOI: 10.1109/HST.2016.7495573.

[108] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "8.1 Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2017, pp. 142–143. DOI: 10.1109/ISSCC.2017.7870301.

[109] S. Mangard, "Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness," en, in *Topics in Cryptology – CT-RSA 2004*, Springer, Berlin, Heidelberg, Feb. 2004, pp. 222–235, ISBN: 978-3-540-20996-6 978-3-540-24660-2. DOI: 10.1007/978-3-540-24660-2_18.

[110] O. X. Standaert et al., "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006, ISSN: 0018-9219. DOI: 10.1109/JPROC.2005.862437.

[111] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," en, in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed., ser. Lecture Notes in Computer Science, Springer Berlin Heidelberg, 1999, pp. 388–397, ISBN: 978-3-540-48405-9.

[112] K. G. et al., "Electromagnetic Analysis: Concrete Results," en, in *CHES 2001*, May 2001, pp. 251–261, ISBN: 978-3-540-42521-2 978-3-540-44709-2. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-44709-1_21.

[113] C. Ramsay and J. Lohuis, "TEMPEST attacks against AES," Fox IT, Tech. Rep., 2017. [Online]. Available: https://resources.fox-it.com/rs/170-CAK-271/images/Tempest_attacks_against_AES.pdf.

[114] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine, "Checking Robustness Against EM Side-Channel Attacks Prior to Manufacturing," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1–1, 2021, Conference Name: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, ISSN: 1937-4151. DOI: 10.1109/TCAD.2021.3092297.

[115] M. Nath, D. Das, and S. Sen, "A Multipole Approach Toward On-Chip Metal Routing for Reduced EM Side-Channel Leakage," *IEEE Microwave and Wireless Components Letters*, vol. 31, no. 6, pp. 685–688, Jun. 2021, Conference Name: IEEE Microwave and Wireless Components Letters, ISSN: 1558-1764. DOI: 10.1109/LMWC.2021.3062809.

[116] V. Lomné, P. Maurine, L. Torres, T. Ordas, M. Lisart, and J. Toublanc, "Modeling Time Domain Magnetic Emissions of ICs," en, in *Integrated Circuit and System Design. Power and Timing Modeling, Optimization, and Simulation*, R. van Leuken and G. Sicard, Eds., ser. Lecture Notes in Computer Science, Berlin, Heidelberg: Springer, 2011, pp. 238–249, ISBN: 978-3-642-17752-1. DOI: 10.1007/978-3-642-17752-1_24.

[117] J. Danial, D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing," *IEEE Access*, vol. 8, pp. 173 414–173 427, 2020, Conference Name: IEEE Access, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3025022.

[118] S. Patranabis, D. B. Roy, A. Chakraborty, N. Nagar, A. Singh, D. Mukhopadhyay, and S. Ghosh, "Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications," en, *Journal of Hardware and Systems Security*, vol. 3, no. 2, pp. 103–131, Jun. 2019, ISSN: 2509-3436. DOI: 10.1007/s41635-018-0049-y. [Online]. Available: https://doi.org/10.1007/s41635-018-0049-y.

[119] M. A. K. F, V. Ganesan, R. Bodduna, and C. Rebeiro, "PARAM: A Microprocessor Hardened for Power Side-Channel Attack Resistance," in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Dec. 2020, pp. 23–34. DOI: 10.1109/HOST45689.2020.9300263.

[120] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020, ISSN: 1558-173X. DOI: 10.1109/JSSC.2019.2945944.

[121] W. Yu and S. Köse, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 2, pp. 244–257, Apr. 2018, Conference Name: IEEE Transactions on Emerging Topics in Computing, ISSN: 2168-6750. DOI: 10.1109/TETC.2016.2620382.

[122] C. Auth et al., "A 10nm high performance and low-power CMOS technology featuring 3rd generation FinFET transistors, Self-Aligned Quad Patterning, contact over active gate and cobalt local interconnects," in *2017 IEEE International Electron Devices Meeting (IEDM)*, ISSN: 2156-017X, Dec. 2017, pp. 29.1.1–29.1.4. DOI: 10.1109/IEDM.2017.8268472.

[123] Fox-IT, "TEMPEST attacks against AES," Tech. Rep. [Online]. Available: https://resources.fox-it.com/rs/170-CAK-271/images/Tempest_attacks_against_AES.pdf.

[124] S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32GHz high-throughput charge-recovery AES core with resistance to DPA attacks," in *2015 Symposium on VLSI Circuits (VLSI Circuits)*, ISSN: 2158-5601, 2158-5636, Jun. 2015, pp. C246–C247. DOI: 10.1109/VLSIC.2015.7231274.

[125] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018, ISSN: 0018-9200. DOI: 10.1109/JSSC.2018.2822691.

[126] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the Masked Logic Style MDPL on a Prototype Chip," en, in *Cryptographic Hardware and Embedded Systems - CHES 2007*, ser. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Sep. 2007, pp. 81–94, ISBN: 978-3-540-74734-5 978-3-540-74735-2. DOI: 10.1007/978-3-540-74735-2_6. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-74735-2_6.

[127] B. Yu, X. Li, C. Chen, Y. Sun, L. Wu, and X. Zhang, "An AES chip with DPA resistance using hardware-based random order execution," en, *Journal of Semiconductors*, vol. 33, no. 6, p. 065 009, Jun. 2012, Publisher: IOP Publishing, ISSN: 1674-4926. DOI: 10.1088/1674-4926/33/6/065009. [Online]. Available: https://doi.org/10.1088%2F1674-4926%2F33%2F6%2F065009.

[128] Shamir, Adi, "protecting smart cards from power analysis with detachable power supplies," US6507913B1, Library Catalog: Google Patents, Jan. 2003. [Online]. Available: https://patents.google.com/patent/US6507913B1/en.

[129] S. B. Nasir, S. Sen, and A. Raychowdhury, "A 130nm hybrid low dropout regulator based on switched mode control for digital load circuits," in *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, Sep. 2016, pp. 317–320. DOI: 10.1109/ESSCIRC.2016.7598306.

[130] S. B. Nasir, S. Sen, and A. Raychowdhury, "Switched-Mode-Control Based Hybrid LDO for Fine-Grain Power Management of Digital Load Circuits," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 2, pp. 569–581, Feb. 2018, Conference Name: IEEE Journal of Solid-State Circuits, ISSN: 1558-173X. DOI: 10.1109/JSSC.2017.2767183.

[131] S. B. Nasir, S. Sen, and A. Raychowdhury, "A Reconfigurable Hybrid Low Dropout Voltage Regulator for Wide-Range Power Supply Noise Rejection and Energy-Efficiency Trade-Off," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 12, pp. 1864–1868, Dec. 2018, Conference Name: IEEE Transactions on Circuits and Systems II: Express Briefs, ISSN: 1558-3791. DOI: 10.1109/TCSII.2018.2816949.

[132] T. Musah, J. E. Jaussi, G. Balamurugan, S. Hyvonen, T.-C. Hsueh, G. Keskin, S. Shekhar, J. Kennedy, S. Sen, R. Inti, M. Mansuri, M. Leddige, B. Horine, C. Roberts, R. Mooney, and B. Casper, "A 4–32 Gb/s Bidirectional Link With 3-Tap FFE/6-Tap DFE and Collaborative CDR in 22 nm CMOS," *IEEE Journal of Solid-State Circuits*, vol. 49, no. 12, pp. 3079–3090, Dec. 2014, Conference Name: IEEE Journal of Solid-State Circuits, ISSN: 1558-173X. DOI: 10.1109/JSSC.2014.2348556.

[133] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, San Francisco, CA: IEEE, Feb. 2009, 64–65, 65a, ISBN: 978-1-4244-3458-9. DOI: 10.1109/ISSCC.2009.4977309. [Online]. Available: http://ieeexplore.ieee.org/document/4977309/.

[134] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "25.3 A 128b AES Engine with Higher Resistance to Power and Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low-Dropout Regulator," in *2019 IEEE International Solid- State Circuits Conference - (ISSCC)*, ISSN: 2376-8606, 0193-6530, Feb. 2019, pp. 404–406. DOI: 10.1109/ISSCC.2019.8662344.

[135] Z. Chen, J. Xi, W. Huang, and M. M. F. Yuen, "Stretchable conductive elastomer for wireless wearable communication applications," en, *Scientific Reports*, vol. 7, no. 1, p. 10 958, Sep. 2017, ISSN: 2045-2322. DOI: 10.1038/s41598-017-11392-w. [Online]. Available: https://www.nature.com/articles/s41598-017-11392-w.

[136] X. Huang, T. Leng, M. Zhu, X. Zhang, J. Chen, K. Chang, M. Aqeeli, A. K. Geim, K. S. Novoselov, and Z. Hu, "Highly Flexible and Conductive Printed Graphene for Wireless Wearable Communications Applications," en, *Scientific Reports*, vol. 5, p. 18 298, Dec. 2015, ISSN: 2045-2322. DOI: 10.1038/srep18298. [Online]. Available: https://www.nature.com/articles/srep18298.

[137] J. M. Rabaey, "The Human Intranet–Where Swarms and Humans Meet," *IEEE Pervasive Computing*, vol. 14, no. 1, pp. 78–83, Jan. 2015, ISSN: 1536-1268. DOI: 10.1109/MPRV.2015.20.

[138] M. Hessar, V. Iyer, and S. Gollakota, "Enabling On-body Transmissions with Commodity Devices," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '16, New York, NY, USA: ACM, 2016, pp. 1100–1111, ISBN: 978-1-4503-4461-6. DOI: 10.1145/2971648.2971682. [Online]. Available: http://doi.acm.org/10.1145/2971648.2971682.

[139] T. Yanagida, "Human body communication system and communication device," US7664476 B2, U.S. Classification 455/188.1, 340/539.1, 455/176.1, 340/522, 340/573.1, 455/127.1, 455/168.1; International Classification H04B1/18; Cooperative Classification H04B13/005; European Classification H04B13/00B, Feb. 2010. [Online]. Available: http://www.google.com/patents/US7664476.

[140] K. Hachisuka, A. Nakata, T. Takeda, K. Shiba, K. Sasaki, H. Hosaka, and K. Itao, "Development of wearable intra-body communication devices," *Sensors and Actuators A: Physical*, vol. 105, no. 1, pp. 109–115, Jun. 2003, ISSN: 0924-4247. DOI: 10.1016/S0924-4247(03)00060-8. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0924424703000608.

[141] T. G. Zimmerman, "Personal Area Networks: Near-field Intrabody Communication," *IBM Syst. J.*, vol. 35, no. 3-4, pp. 609–617, Sep. 1996, ISSN: 0018-8670. DOI: 10.1147/sj.353.0609. [Online]. Available: http://dx.doi.org/10.1147/sj.353.0609.

[142] R. Xu, H. Zhu, and J. Yuan, "Electric-Field Intrabody Communication Channel Modeling With Finite-Element Method," *IEEE Transactions on Biomedical Engineering*, vol. 58, no. 3, pp. 705–712, Mar. 2011, ISSN: 0018-9294. DOI: 10.1109/TBME.2010.2093933.

[143] J. Park, H. Garudadri, and P. P. Mercier, "Channel Modeling of Miniaturized Battery-Powered Capacitive Human Body Communication Systems," *IEEE Transactions on Biomedical Engineering*, vol. 64, no. 2, pp. 452–462, Feb. 2017, ISSN: 0018-9294. DOI: 10.1109/TBME.2016.2560881.

[144] N. Cho, J. Yoo, S. Song, J. Lee, S. Jeon, and H. Yoo, "The Human Body Characteristics as a Signal Transmission Medium for Intrabody Communication," *IEEE Transactions on Microwave Theory and Techniques*, vol. 55, no. 5, pp. 1080–1086, May 2007, ISSN: 0018-9480. DOI: 10.1109/TMTT.2007.895640.

[145] Ž. Lucev, I. Krois, and M. Cifrek, "A Capacitive Intrabody Communication Channel from 100 kHz to 100 MHz," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 12, pp. 3280–3289, Dec. 2012, ISSN: 0018-9456. DOI: 10.1109/TIM.2012.2205491.

[146] M. Oberle, "Low power systems-on-chip for biomedical applications," en, Doctoral Thesis, ETH Zurich, 2002. DOI: 10.3929/ethz-a-004379615. [Online]. Available: https://www.research-collection.ethz.ch/handle/20.500.11850/146680.

[147] M. S. Wegmueller, M. Oberle, N. Felber, N. Kuster, and W. Fichtner, "Signal Transmission by Galvanic Coupling Through the Human Body," *IEEE Transactions on Instrumentation and Measurement*, vol. 59, no. 4, pp. 963–969, Apr. 2010, ISSN: 0018-9456. DOI: 10.1109/TIM.2009.2031449.

[148] J. Bae, H. Cho, K. Song, H. Lee, and H. Yoo, "The Signal Transmission Mechanism on the Surface of Human Body for Body Channel Communication," *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 3, pp. 582–593, Mar. 2012, ISSN: 0018-9480. DOI: 10.1109/TMTT.2011.2178857.

[149] M. A. Callejón, D. Naranjo-Hernández, J. Reina-Tosina, and L. M. Roa, "A Comprehensive Study Into Intrabody Communication Measurements," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 9, pp. 2446–2455, Sep. 2013, ISSN: 0018-9456. DOI: 10.1109/TIM.2013.2258766.

[150] M.-F. Wong and J. Wiart, "Modelling of electromagnetic wave interactions with the human body," *Comptes Rendus Physique*, Interaction of electromagnetic fields with the environment, vol. 6, no. 6, pp. 585–594, Jul. 2005, ISSN: 1631-0705. DOI: 10.1016/j.crhy.2005.07.003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1631070505000800.

[151] J. W. Hand, "Modelling the interaction of electromagnetic fields (10 MHz-10 GHz) with the human body: Methods and applications," eng, *Physics in Medicine and Biology*, vol. 53, no. 16, R243–286, Aug. 2008, ISSN: 0031-9155. DOI: 10.1088/0031-9155/53/16/R01.

[152] R. Augustine, "Electromagnetic modelling of human tissues and its application on the interaction between antenna and human body in the BAN context," en, Ph.D. dissertation, Université Paris-Est, Jul. 2009. [Online]. Available: https://tel.archives-ouvertes.fr/tel-00499255/document.

[153] B. Kibret, A. K. Teshome, and D. T. H. Lai, "Human Body as Antenna and its Effect on Human Body Communications," English, *Progress In Electromagnetics Research*, vol. 148, pp. 193–207, 2014, ISSN: 1070-4698. DOI: 10.2528/PIER14061207. [Online]. Available: http://www.jpier.org/PIER/pier.php?paper=14061207.

[154] S. Sen, "Invited: Context-aware energy-efficient communication for IoT sensor nodes," in *2016 53nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, Jun. 2016, pp. 1–6. DOI: 10.1145/2897937.2905005.

[155] H. Cho, H. Kim, M. Kim, J. Jang, Y. Lee, K. J. Lee, J. Bae, and H. J. Yoo, "A 79 pJ/b 80 Mb/s Full-Duplex Transceiver and a $42.5;upmutextW$ 100 kb/s Super-Regenerative Transceiver for Body Channel Communication," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 1, pp. 310–317, Jan. 2016, ISSN: 0018-9200. DOI: 10.1109/JSSC.2015.2498761.

[156] S. Maity, B. Chatterjee, G. Chang, and S. Sen, "A 6.3pJ/b 30Mbps -30dB SIR-tolerant Broadband Interference-Robust Human Body Communication Transceiver using Time Domain Signal-Interference Separation," 2018.

[157] S. Sen, J. Koo, and S. Bagchi, "TRIFECTA: Security, Energy Efficiency, and Communication Capacity Comparison for Wireless IoT Devices," *IEEE Internet Computing*, vol. 22, no. 1, pp. 74–81, Jan. 2018, Conference Name: IEEE Internet Computing, ISSN: 1941-0131. DOI: 10.1109/MIC.2018.011581520.

[158] B. Chatterjee, A. Srivastava, D.-H. Seo, D. Yang, and S. Sen, "A Context-aware Reconfigurable Transmitter with 2.24 pJ/bit, 802.15.6 NB-HBC and 4.93 pJ/bit, 400.9 MHz MedRadio Modes with 33.6% Transmit Efficiency," in *2020 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, ISSN: 2375-0995, Aug. 2020, pp. 75–78. DOI: 10.1109/RFIC49505.2020.9218344.

[159] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They Can Hear Your Heartbeats: Non-invasive Security for Implantable Medical Devices," in *Proceedings of the ACM SIGCOMM 2011 Conference*, ser. SIGCOMM '11, New York, NY, USA: ACM, 2011, pp. 2–13, ISBN: 978-1-4503-0797-0. DOI: 10.1145/2018436.2018438. [Online]. Available: http://doi.acm.org/10.1145/2018436.2018438.

[160] R. M. Fish and L. A. Geddes, "Conduction of electrical current to and through the human body: A review," eng, *Eplasty*, vol. 9, e44, Oct. 2009, ISSN: 1937-5719.

[161] Y. A. Chizmadzhev, A. V. Indenbom, P. I. Kuzmin, S. V. Galichenko, J. C. Weaver, and R. O. Potts, "Electrical properties of skin at moderate voltages: Contribution of appendageal macropores.," *Biophysical Journal*, vol. 74, no. 2 Pt 1, pp. 843–856, Feb. 1998, ISSN: 0006-3495. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1302564/.

[162] J. Rosell, J. Colominas, P. Riu, R. Pallas-Areny, and J. G. Webster, "Skin impedance from 1 Hz to 1 MHz," eng, *IEEE transactions on bio-medical engineering*, vol. 35, no. 8, pp. 649–651, Aug. 1988, ISSN: 0018-9294. DOI: 10.1109/10.4599.

[163] *Lecture Notes | Electromagnetic Energy: From Motors to Lasers | Electrical Engineering and Computer Science | MIT OpenCourseWare*, en. [Online]. Available: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-007-electromagnetic-energy-from-motors-to-lasers-spring-2011/lecture-notes/.

[164] J. Larsson, "Electromagnetics from a quasistatic perspective," *American Journal of Physics*, vol. 75, no. 3, pp. 230–239, Feb. 2007, ISSN: 0002-9505. DOI: 10.1119/1.2397095. [Online]. Available: https://aapt.scitation.org/doi/full/10.1119/1.2397095.

[165] S. Gabriel, R. W. Lau, and C. Gabriel, "The dielectric properties of biological tissues: III. Parametric models for the dielectric spectrum of tissues," en, *Physics in Medicine & Biology*, vol. 41, no. 11, p. 2271, 1996, ISSN: 0031-9155. DOI: 10.1088/0031-9155/41/11/003. [Online]. Available: http://stacks.iop.org/0031-9155/41/i=11/a=003.

[166] H. A. Haus and M. R. James, *Electromagnetic Fields and Energy*. Prentice-Hall: Englewood Cliffs, NJ, 1989. (Massachusetts Institute of Technology: MIT OpenCourseWare). http://ocw.mit.edu, ISBN: 978-0-13-249020-7. [Online]. Available: (Massachusetts%20Institute%20of%20Technology:%20MIT%20OpenCourseWare).%20http://ocw.mit.edu.

[167] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, Dec. 2015, ISSN: 0163-6804. DOI: 10.1109/MCOM.2015.7355562.

[168] M. Nath, S. Maity, and S. Sen, "Toward Understanding the Return Path Capacitance in Capacitive Human Body Communication," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 10, pp. 1879–1883, Oct. 2020, Conference Name: IEEE Transactions on Circuits and Systems II: Express Briefs, ISSN: 1558-3791. DOI: 10.1109/TCSII.2019.2953682.

[169] S. Sen, "SocialHBC: Social Networking and Secure Authentication Using Interference-Robust Human Body Communication," in *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*, ser. ISLPED '16, New York, NY, USA: ACM, 2016, pp. 34–39, ISBN: 978-1-4503-4185-1. DOI: 10.1145/2934583.2934609. [Online]. Available: http://doi.acm.org/10.1145/2934583.2934609.

[170] S. Sen, "Human body communication interference rejection system," US20190379414A1, Dec. 2019. [Online]. Available: https://patents.google.com/patent/US20190379414A1/en.

[171] P. Mehrotra, S. Maity, and S. Sen, "An Improved Update Rate CDR for Interference Robust Broadband Human Body Communication Receiver," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 13, no. 5, pp. 868–879, Oct. 2019, Conference Name: IEEE Transactions on Biomedical Circuits and Systems, ISSN: 1940-9990. DOI: 10.1109/TBCAS.2019.2940746.

[172] "IEEE Standard for Safety Levels With Respect to Human Exposure to Electromagnetic Fields, 0-3 kHz," *IEEE Std C95.6-2002*, pp. 1–, Oct. 2002. DOI: 10.1109/IEEESTD.2002.94143.

[173] "IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz," *IEEE Std C95.1-2005 (Revision of IEEE Std C95.1-1991)*, pp. 1–238, Apr. 2006. DOI: 10.1109/IEEESTD.2006.99501.

[174] *Worker Deaths by Electrocution: A Summary of NIOSH Surveillance and Investigative Findings*, en. National Institute for Occupational Saftey and Health, 1998.

[175] *File:Skin.png*, en. [Online]. Available: https://en.wikipedia.org/wiki/File:Skin.png.

[176] S. Maity, M. Nath, G. Bhattacharya, B. Chatterjee, and S. Sen, "On the Safety of Human Body Communication," *IEEE Transactions on Biomedical Engineering*, vol. 67, no. 12, pp. 3392–3402, Dec. 2020, Conference Name: IEEE Transactions on Biomedical Engineering, ISSN: 1558-2531. DOI: 10.1109/TBME.2020.2986464.

[177] M. Nath, S. Maity, S. Avlani, S. Weigand, and S. Sen, "Inter-body coupling in electro-quasistatic human body communication: Theory and analysis of security and interference properties," en, *Scientific Reports*, vol. 11, no. 1, p. 4378, Feb. 2021, ISSN: 2045-2322. DOI: 10.1038/s41598-020-79788-9. [Online]. Available: https://www.nature.com/articles/s41598-020-79788-9.

[178] S. Avlani, M. Nath, S. Maity, and S. Sen, "A 100KHz-1GHz Termination-dependent Human Body Communication Channel Measurement using Miniaturized Wearable Devices," in *2020 Design, Automation Test in Europe Conference Exhibition (DATE)*, ISSN: 1558-1101, Mar. 2020, pp. 650–653. DOI: 10.23919/DATE48585.2020.9116556.

[179] A. Datta, M. Nath, D. Yang, and S. Sen, "Advanced Biophysical Model to Capture Channel Variability for EQS Capacitive HBC," *IEEE Transactions on Biomedical Engineering*, pp. 1–1, 2021, Conference Name: IEEE Transactions on Biomedical Engineering, ISSN: 1558-2531. DOI: 10.1109/TBME.2021.3074138.

[180] S. Maity, B. Chatterjee, G. Chang, and S. Sen, "BodyWire: A 6.3-pJ/b 30-Mb/s −30-dB SIR-Tolerant Broadband Interference-Robust Human Body Communication Transceiver Using Time Domain Interference Rejection," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 10, pp. 2892–2906, Oct. 2019, Conference Name: IEEE Journal of Solid-State Circuits, ISSN: 1558-173X. DOI: 10.1109/JSSC.2019.2932852.

[181] A. Datta et al., "In-body to out-of-body communication channel modeling for ruminant animals for smart animal agriculture," in *IEEE EMBC*, 2021.

[182] S. Sriram, S. Avlani, M. P. Ward, and S. Sen, "Electro-Quasistatic Animal Body Communication for Chronic Untethered Rodent Biopotential Recording," *arXiv:2005.05370 [cs, eess]*, May 2020, arXiv: 2005.05370. [Online]. Available: http://arxiv.org/abs/2005.05370.

[183] S. Maity, N. Modak, D. Yang, S. Avlani, M. Nath, J. Danial, D. Das, P. Mehrotra, and S. Sen, "A 415 nW Physically and Mathematically Secure Electro-Quasistatic HBC Node in 65nm CMOS for Authentication and Medical Applications," in *2020 IEEE Custom Integrated Circuits Conference (CICC)*, ISSN: 2152-3630, Mar. 2020, pp. 1–4. DOI: 10.1109/CICC48029.2020.9075930.

[184] M. Nath, A. K. Ulvog, S. Weigand, and S. Sen, "Understanding The Role of Magnetic and Magneto-Quasistatic Fields in Human Body Communication," *arXiv:2011.00125 [physics]*, Oct. 2020, arXiv: 2011.00125. [Online]. Available: http://arxiv.org/abs/2011.00125.

[185] B. Chatterjee, G. K. K, M. Nath, S. Xiao, D. Das, J. Krishna, and S. Sen, "A 1.15uw 5.75mm3 implant with a bidirectional neural sensor and stimulator soc utilizing biphasic quasi-static brain communication achieving 6kbps-10mbps uplink with compressive sensing and ro-puf based collision avoidance," in *2021 IEEE Symposia on VLSI Technology and Circuits*, 2021.

[186] J. Blackstone, D. Das, A. Althoff, S. Sen, and R. Kastner, "Istellar: Intermittent signature attenuation embedded crypto with low-level metal routing," in *2021 IEEE/ACM ICCAD*, 2021.

[187] S. Ghosh, D. Das, C. Tokunaga, A. L. Varna, and J. Friel, "Countermeasures against hardware side-channel attacks on cryptographic operations," US20190318130A1, Oct. 2019. [Online]. Available: https://patents.google.com/patent/US20190318130A1/en.

[188] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-stellar: An em/power sca-resilient aes-256 with synthesizable signature attenuation," in *under review*, 2021.

[189] A. Ghosh, D. Das, S. Ghosh, and S. Sen, "Synthesizable switch capacitor-based time-varying transfer function for fcn and cnn ml-sca attack-resistant aes256 in 65nm cmos," in *under review*, 2021.

[190] A. Ghosh, D. Das, and S. Sen, "Em self-awareness and resilience with single on-chip loop: Leakage sensing, attack detection and protection," in *under review*, 2021.

[191] A. Golder, B. Ma, D. Das, J. Danial, S. Sen, and A. Raychowdhury, "120.147 Efficient Electromagnetic Side Channel Analysis by Probe Positioning using Multi-Layer Perceptron," Tech. Rep. 988, 2020. [Online]. Available: https://eprint.iacr.org/2020/988.

[192] D.-H. Seo, M. Nath, D. Das, B. Chatterjee, S. Ghosh, and S. Sen, "PG-CAS: Patterned-Ground Co-planar Capacitive Asymmetry Sensing for mm-range EM Side-channel Attack Probe Detection," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, ISSN: 2158-1525, May 2021, pp. 1–5. DOI: 10.1109/ISCAS51556.2021.9401580.

[193] D. Seo, M. Nath, D. Das, S. Ghosh, and S. Sen, "Enhanced Detection Range for EM Side-channel Attack Probes utilizing Co-planar Capacitive Asymmetry Sensing," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, 2021.

[194] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "An EM/Power SCA Resilient AES-256 with Synthesizable Signature Attenuation using Digital-Friendly Current Source and RO-Bleed based Integrated Local Feedback and Global Switched Mode Control," in *2021 IEEE International Solid- State Circuits Conference - (ISSCC)*, 2021.

[195] A. Ghosh, D. Das, and S. Sen, "Physical Time-Varying Transfer Functions as Generic Low-Overhead Power-SCA Countermeasure," Tech. Rep. 317, 2020. [Online]. Available: https://eprint.iacr.org/2020/317.

[196] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "36.2 An EM/Power SCA-Resilient AES-256 with Synthesizable Signature Attenuation Using Digital-Friendly Current Source and RO-Bleed-Based Integrated Local Feedback and Global Switched-Mode Control," in *2021 IEEE International Solid- State Circuits Conference (ISSCC)*, ISSN: 2376-8606, vol. 64, Feb. 2021, pp. 499–501. DOI: 10.1109/ISSCC42613.2021.9365978.

A. RESOURCES

Here is the list of open source codes, datasets, and video demonstrations released related to this thesis:

- `X-DeepSCA` Attack Codes & Dataset: https://github.com/SparcLab/X-DeepSCA
- EM/Power SCA Countermeasure Demonstration Video: https://www.youtube.com/watch?v=sh5_SWM7o_U&list=PLV45P77Yo8yf3nm5-LDQVZLZ6sWJOFZWq
- Evaluation of CDSA against advanced ML SCA attacks: https://www.youtube.com/watch?v=J9TWTV8sXyM&list=PLV45P77Yo8yf3nm5-LDQVZLZ6sWJOFZWq
- STELLAR Summary Video (HOST 2019): https://www.youtube.com/watch?v=BsUlWuFapoM&list=PLV45P77Yo8yf3nm5-LDQVZLZ6sWJOFZWq
- SCNIFFER Demonstration Video: https://www.youtube.com/watch?v=5aVkcgyDJdE&list=PLV45P77Yo8yf3nm5-LDQVZLZ6sWJOFZWq
- SCNIFFER Scripts: https://github.com/SparcLab/SCNIFFER
- Synthesizable STELLAR Scripts: https://github.com/SparcLab/Syn-STELLAR
- Synthesizable STELLAR Demonstration Video: https://www.youtube.com/watch?v=DvmNUciMst4&list=PLV45P77Yo8yf3nm5-LDQVZLZ6sWJOFZWq

VITA

Debayan Das is a Ph.D. student in Electrical and Computer Engineering at Purdue University, working with Professor Shreyas Sen. He received his Bachelor of Electronics and Telecommunication Engineering from Jadavpur University, India, in 2015. Prior to joining PhD, he worked as an Analog Design Engineer at a start-up based in India. He has interned with the Security Research Lab, Intel Labs, OR, over the summers of 2018 and 2020. His research interests include mixed-signal IC design and hardware security.

Debayan was a recipient of the IEEE HOST Best Student Paper Award in 2017, 2019, IEEE CICC Best Student Paper Award in 2021, the 3rd Best Poster Award in IEEE HOST 2018, and the 2nd Best Demo Award in HOST 2020. 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 was recognized as the winner (third place) of the ACM ICCAD 2020 Student Research Competition (SRC). During his PhD, he has been awarded the ECE fellowship during 2016-18, the SSCS Pre-doctoral Achievement Award in 2020-21, and the Bilsland Dissertation Fellowship during the final year (2020-21) for his outstanding overall achievements. In 2021, he received the Outstanding Graduate Research Award by the Purdue University College of Engineering for demonstrating excellence and leadership in research. He has authored/co-authored more than 40 peer-reviewed conferences and journals including 2 book chapters and 1 US patent. He has been serving as a primary reviewer for multiple reputed journals and conferences including TCAS-I, TCAD, TVLSI, TODAES, IEEE Access, IoTJ, JETCAS, TIFS, Design & Test, MWCL, IEEE Solid-State Circuits Letters, Consumer Electronics Magazine, IET Computers & Digital Techniques, IEEE Sensors Letters, IEEE Security & Privacy.