ENHANCING SIDE CHANNEL SECURITY WITH FULLY INTEGRATED INDUCTIVE VOLTAGE REGULATORS

A Dissertation
Presented to
The Academic Faculty

By

Monodeep Kar

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of School of Electrical and Computer Engineering

Georgia Institute of Technology

August 2017

ENHANCING SIDE CHANNEL SECURITY WITH FULLY INTEGRATED INDUCTIVE VOLTAGE REGULATORS

Approved by:

Dr. Saibal Mukhopadhyay
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Raheem Beyah
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Arijit Raychowdhury
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Vivek De
Intel Fellow, Director of Circuit Technology Research, Architecture & Design Research (ADR), Intel Labs, Hillsboro, Oregon
Intel Corporation

Dr. Satish Kumar
The George W. Woodruff School of Mechanical Engineering
Georgia Institute of Technology

Date Approved: June 29, 2017

To my parents, Chirasree Kar and Nirmal Kar.

ACKNOWLEDGEMENTS

My PhD years have been one of the best phases of my life and I would like to take this opportunity to express my gratitude for the people who have contributed to and encouraged me in this work.

I would like to acknowledge and express the highest gratitude to my advisor, Prof. Saibal Mukhopadhyay. He has been a constant source of inspiration and support to try out new ideas and push the boundaries of research. I am thankful to him for his motivation and guidance on this project which I started without any background knowledge and providing the resources necessary to succeed. From him, I have gained not only technical expertise, but also an understanding of managing technology development and presenting research effectively. I am also thankful to him for never letting me worry about the next source of funding and numerous trips to conferences all around the USA and the world.

I would like to thank Prof. Raheem Beyah, Prof. Arijit Raychowdhury, Prof. Satish Kumar and Dr. Vivek De for being part of my thesis committee. Their valuable inputs played a major role in shaping my final thesis.

I am grateful to Sanu Mathew, Anand Rajan, and Vivek De who were my collaborators at Intel Labs, for providing guidance and valuable insights for this project and demonstrating a sincere interest on success of this project. I would like to thank NSF, SRC and Intel Corporation for providing funding for this project.

I feel fortunate to spend two semesters during my PhD at Kilby Labs, Texas Instruments and Intel Labs. I would like to thank all the mentors at my internships, Saurav Bandopadhyay and Jeffery Morroni at Kilby and Sudhir Satpathy, Vikram Suresh, Sanu Mathew and Ram Krishnamurthy at Intel Labs, for allowing me to work on cutting edge research, providing important technical and professional suggestions and teaching me how to present ideas in a simple yet effective manner. I would also like to take this opportunity to thank Prof. Tushar Krishna, He Xiao and Nitish Kumar for collaborating on several research

projects and teaching me topics outside my area of expertise.

I would like to thank all members in GREEN Lab, Georgia Tech for their guidance, friendship, and support. Subho Chatterjee, Amit Trivedi, Denny Lie, Boris Alexandrov, Wen Yueh, Khondker Zakir Ahmed, Sergio Carlo and Krishna Yeleswarapu for introducing me to the lab, starting me off on the right foot and the many wonderful coffee breaks and meals. I would like to thank all the present Green Lab members for their valuable discussions and insights; Jaeha Kung, Duckhwan Kim, Faisal Amir, Arvind Singh, Jong Hwan Ko, Taesik Na, Yun Long, Burhan Mudassar, Chaitanya Krishna and Edward Lee. Especially, I am thankful to Khondker Zakir Ahmed and Sergio Carlo for teaching me how to fabricate a chip from the ground up and Arvind Singh for being a great teammate for many research projects. I will never forget the moments spent with my colleagues and I look forward to meeting them in future again.

I want to thank all of my teachers, both at Georgia Tech and IIT Kharagpur, whose classes helped me better understand the various topics in Electrical and Computer Engineering. I would also like to take this opportunity to thank Keith May, Pamela Halverson, Daniela Staiculescu, and Tasha Torrence for their technical and administrative support.

I would like to thank all my close friends in Atlanta and the US, including my flatmates for the last 5 years, folks at 1033 Tumlin and Homepark Area, the afternoon coffee crew, colleagues in the Klaus building, CRC buddies, friends from my undergrad days and the people I met at Hillsboro and Dallas during my internships, for all the amazing and memorable times. Thanks for the wonderful meals, trips, gatherings, and stimulating discussions. I have had a special rapport with each one of you personally and I cherish that bond.

Last but foremost, I would like to thank my parents for the unconditional love and support they have given me over the course of my life. I wouldn't have made it this far without their support during the course of the PhD, particularly at tough times during tapeouts and deadlines. It is the difficult decisions and sacrifices that they have made, that has brought me to the position I am in right now, and for that I am eternally thankful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

The energy-efficiency and security needs in computing systems, ranging from high performance processors to low-power devices are steadily increasing. State-of-the-art digital systems use dedicated encryption hardware for compute intensive steps requiring encryption. These encryption engines are vulnerable to different forms of side channel attacks (SCA). Traditional countermeasures to protect against such attacks suffer from high power and performance overheads, diminishing system energy-efficiency. Integrated voltage regulators (IVR) are an integral part of energy-efficient digital systems. As inductive IVRs isolate the side channel signatures of an encryption engine from the measured side channel signatures at the IVR input, they can be potentially exploited for improvement in power SCA (PSCA) resistance. Moreover the presence of an inductance, a strong electromagnetic (EM) radiator, in an inductive IVR can potentially improve EMSCA resistance as well. This thesis investigates the design of an inductive IVR for improving side channel resistance of an encryption engine.

The IVR transformations that modify the side channel signatures from an encryption engine are identified and a simulation framework is used to quantify the improvement in PSCA resistance at the input of an illustrative IVR. A test-chip, containing an all-digital IVR architecture, a security aware block called Loop Randomization (LR) inside the IVR and a 128-bit Advanced Encryption Standard (AES) engine is fabricated in 130nm CMOS. Measurement results from the test-chip with an active LR demonstrates improved resistance to a Correlation Power Attack (CPA) and no leakage in Test Vector Leakage Assessment (TVLA) in the power signature at the IVR input. The proposed security aware IVR design also improves system EMSCA resistance, quantified through CPA and TVLA. The proposed security aware IVR design modifications are all-digital, synthesizable, seamlessly integrable into the existing IVR architectures and incurs minimal overhead on the system area/power/performance.

CHAPTER 1
INTRODUCTION

Emergence of ubiquitous computing has surrounded our lives with a massive amount of gadgets, the data processed and communicated by them and their decision making. As these devices, ranging from high performance processors to ultra-low power wireless nodes, are seamlessly integrated in our lives, security is becoming an important aspect to reconsider for the design of these systems. High-performance processors like Intel Haswell/Skylake [1], IBM z9/z10 [2, 3], ARM A-64 instruction set architecture, SPARK SoC and other processors [4] support secure execution of programs. Intel's secure guard extension (SGX) provides integrity and confidentiality guarantees to security sensitive computation performed on a computer leveraging the encryption hardware in the remote computer [5]. Most of these aforementioned processors also use dedicated on-chip encryption accelerators to improve energy-efficiency and throughput for bulk encryption events which include rapid memory and data encryption. Adding intelligence to low power compute nodes and sensors involves exchanging sensitive information through insecure channel. The transmission of data packets through the channel has to be encrypted to prevent any adversary from snooping to the broadcast packets. However use of a strong encryption scheme is not enough to secure these systems from a hostile environment during operation. A wide class of hardware attacks, for example a *side channel attack (SCA)*, can break the hardware implementation of the encryption engine used in such systems.

A SCA exploits various physical quantities like power consumption of the system, electromagnetic radiation and acoustic measurements, to deduce relevant information about the underlying computation of the system [6, 7, 8, 9, 10, 11, 12, 13]. Different forms of SCAs are appearing as significant threats to the security of a range of hardware platforms. An adversary exploits the correlation between the measured side channel data and a targeted

step in the algorithm to find out partial or complete information about the underlying algorithm, for example key used in a series of encryption. Preventing the side channels from leaking information about the underlying computation has been studied in details for past two decades [14, 9, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30]. These techniques, commonly referred to as *countermeasures*, tries to hide or mask the patterns correlated to the concurrent computation from appearing in the side channel measurement. However the largest drawback of these countermeasures are their power, area and/or performance overhead, which significantly reduces the energy-efficiency of the overall platform and the added effort in the design-modification resulting in higher time-to-market-delay.

Improving energy-efficiency of digital systems has been one of the major research thrust over the last decade [31, 32, 33, 1]. Several circuit techniques like power gating, clock gating, dynamic voltage-frequency scaling (DVFS) [34] and on-chip voltage regulation [35, 36] have been introduced in digital circuits to improve energy efficiency of increasingly complex computations. Encryption algorithm specific techniques like use of GF($(2^4)^2$) field [37] and area-optimized encrypt and decrypt Galois-field polynomial [38] for AES computation have been used for improvement in energy-efficiency. Unfortunately a trade-off exists between improving resistance to SCA through the traditional countermeasures and improving energy-efficiency, as the power and performance overhead of the countermeasures hurt a high performance processor in its throughput requirement as well as a resource constrained system in its energy consumption. The encryption algorithm specific techniques [39] have been linked to increased vulnerability to side channel attacks [40]. Designing energy-efficient and secure digital platforms is a key challenge to address in a world with connected devices.

Voltage regulators integrated into the same die as the digital logic, referred to as Integrated Voltage Regulators (IVRs) have been demonstrated to improve energy efficiency of digital processors [41, 1, 42, 35, 43, 44, 45, 46, 47]. Integration of voltage regulators achieve fast transitions of processor supply voltage between power-states which maximizes

the benefits of DVFS and improves the transient response of supply voltage to dynamic load current transitions. An inductive IVR integrates the power stage of an inductive buck converter with the digital logic in the same die and have been demonstrated in commercial processors like Intel's Haswell [1]. As the inductive IVR isolates the supply of the digital processor from the supply of the IVR, it can be potentially exploited for improvement in side channel resistance.

1.1 Problem Statement

The goal of this research is to investigate the impact of a fully integrated inductive IVR and required design modifications on improving side channel attack resistance of encryption engines. This includes

- Identifying different transformations through an inductive IVR affecting side channel attack resistance of an encryption engine
- Security aware design modifications in an IVR to improve side channel attack resistance
- Characterizing improvement in power and EM side channel attack resistance through measurement from a prototype test-chip

1.2 Organization of this thesis

Chapter 2 provides a detailed literature survey of integrated voltage regulators, inductor integration technologies and existing techniques for integration of inductive IVR into an advanced digital process. Different categories of existing countermeasures are also discussed along with area/power/performance overheads of selected countermeasures.

Chapter 3 identifies the key transformations between the load current signatures to the input current signature of an inductive IVR. A simulation framework is proposed for generating and analyzing time domain PSCA signatures of an AES engine and an inductive

IVR. The impact of the IVR transformations are quantified through a correlation study on an illustrative IVR design driving a 128-bit AES engine as well as resistance to CPA at the input of the illustrative IVR. The impact of selected design parameters of the IVR on CPA resistance at the IVR input are provided. Two alternative attack modalities are used to evaluate CPA resistance at the IVR input.

Chapter 4 describes design of an all-digital architecture of a fully integrated inductive IVR which is suitable for integration in an advanced digital process. Measurement results from a 130nm testchip is demonstrated.

Chapter 5 presents characterization of PSCA resistance using measured data from the 130nm test-chip consisting of the inductive IVR, described in chapter 4, driving a 128 bit AES engine. Two statistical tests are performed: CPA and Test Vector Leakage Assessment (TVLA) which is a leakage detection test. Post-processing steps which were used for analysis are discussed in detail.

Chapter 6 describes a new circuit which randomizes the control loop of the IVR for enhancing the PSCA resistance at the IVR input. The impact of the randomization on IVRs stability, PSCA resistance of the system and area/power/performance overheads on the system are elaborated.

Chapter 7 evaluates the role of an inductive IVR in improving EM side channel resistance, by exploiting strong EM emission from the IVR's inductors. Different EM probes are used to understand EM leakage from the designed test-chip. Results for the baseline design as well as with active loop randomization is presented.

Chapter 8 summarizes the contribution of this thesis and provides a brief discussion on future research direction.

CHAPTER 2

BACKGROUND

2.1 Integrated Voltage Regulators

A processor/SoC requires multiple independent voltage domains to maximize energy efficiency through DVFS [1, 44]. Traditional power-delivery solutions use on-board voltage-regulator-modules (VRM) to supply these voltage domains. Therefore, increasing number of independent voltage rails significantly increases the area required by the on-board VRMs, reducing the system power density. Moreover the overall system power efficiency degrades due to power loss across the PCB traces carrying supply current from the on-board VRMs to the chip. IVRs integrate a voltage-regulator (VR) with the digital logic in the same die and boost achievable independent on-chip voltage domains as well as increase the power density of the system by reducing form factor.

The largest roadblock in the integration of VRs, in particular switching VRs, has been passive integration. Existing well-known VR topologies for down-conversion can be largely classified into three categories, namely low dropout regulators (LDO), switched-capacitor regulators (SCVRs) and inductive buck regulators. LDOs have been predominantly the first choice for fine-grain on-chip voltage regulation [48, 46] due to 1) lower capacitance usage than SCVRs and 2) seamless regulation for a wide range of output voltage and current, without any steady state switching disturbances at the output. However the largest challenge with LDOs has been their power efficiency, which scales with output voltage. SCVRs and inductive buck regulators are switching converters and requires output capacitance to achieve a lower output ripple. Integration of SCVRs and inductive buck regulators has been achieved by increasing the switching frequency beyond 50MHz [43, 49, 50, 51, 41, 52, 53, 54, 55]. Integration of SCVRs with digital cores has been demonstrated in [35, 36,

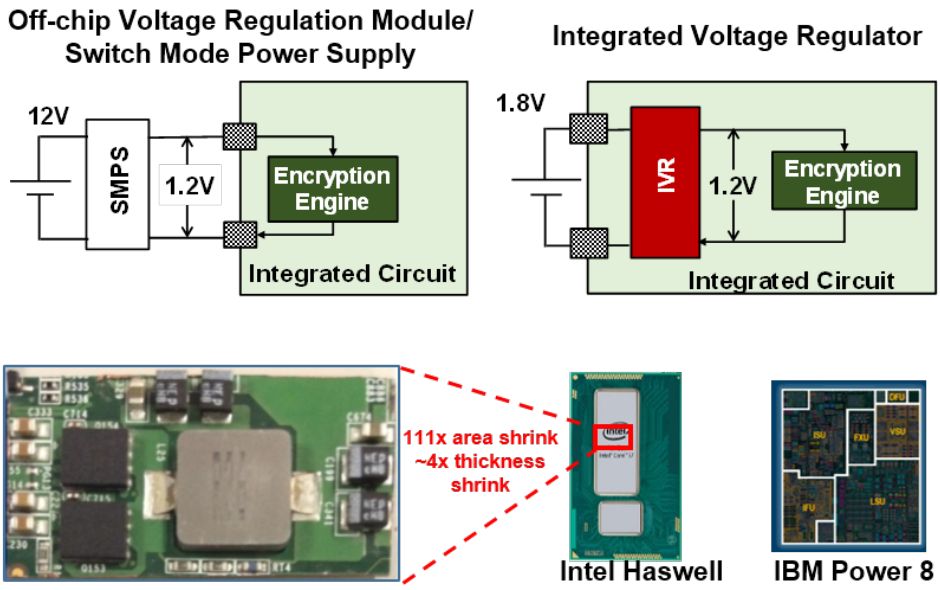

Figure 2.1: Commercial processors ([1, 44]) with IVRs and the corresponding volume shrinkage of the power delivery architecture, source: http://www.psma.com/sites/default/files/uploads/tech-forums-packaging/presentations/is87-package-and-platform-view-intel%E2%80%99s-fully-integrated-coltage-regulator.pdf

56]. Higher capacitance density at advanced process nodes helps full on-chip integration of the SCVRs [57]. SCVRs show better power efficiency than LDOs particularly at low and medium output voltage levels. However the power efficiency of a SCVR maximizes when the regulation voltage is closer to its theoretical conversion ratio, which depends on the SCVR topology. The largest advantage of an inductive IVR over a LDO or a SCVR is its seamless regulation at different output voltages without loss of power efficiency. However, integration of inductance has matured at a much slower pace than on-chip capacitance.

2.1.1 Integration of on-chip/on-package inductance

Integrating inductance with high quality factor has received a lot of attention in the last decade. Fig. 2.2 shows several forms of integrated inductance that has been used in IVRs. On-chip spiral inductance have been used in [58], however, one of the largest challenges in using on-chip inductance is high effective resistance, contributed by both the DC and

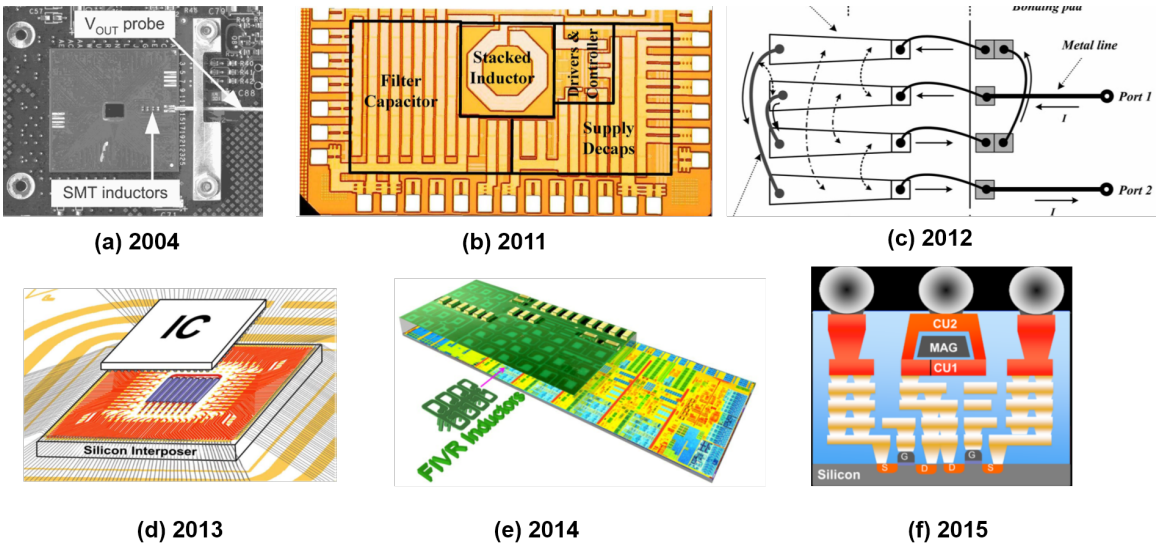

Figure 2.2: Evolution of integrated inductor technologies (a) Hazucha et. al [54] (b)Kudva et. al. [58] (c)Ahn. et. al. [49] (d) Burton et. al. [41] (e)Sturcken et. al. [59] (f) Sturcken et. al. [60]

AC resistance. This leads to a low quality factor (Q_L) and therefore low power efficiency. Hazucha et. al. in [54] used air-core package inductance for realizing a high frequency power stage. Package bondwires offer relatively higher inductance value than on-chip inductance and have been used in inductive IVRs [49, 52, 53, 43, 61]. Recently published works report magnetic interposer [59], magnetic thin film [60], on-chip solenoid [55] and embedded magnetic core inductors [62] achieving higher inductance density than the traditional on-chip spiral or package inductors.

2.1.2 Controller Design for IVR

Use of smaller passives and higher switching frequency (both in SCVRs and inductive VRs) allows switching IVRs to achieve higher unity gain frequency (UGF) of the voltage conversion stage. However to achieve a higher bandwidth of the overall loop (voltage conversion stage + controller), the controller needs to have a bandwidth of similar order.

A higher bandwidth of the overall control loop translates to faster recovery from dynamic load current or supply voltage transients and faster settling time for a reference/power-state transient. Hysteretic/PFM control has been widely used in high frequency VRs due to their ease of implementation, guaranteed stability and fast response [50, 54]. However load current dependent hysteresis frequency and larger output ripple make hysteretic controllers unattractive for a range of applications. Traditional pulse width modulation (PWM) control, both analog and digital, can solve the aforementioned issues, however, achieving a high bandwidth is particularly challenging for analog PWM controllers in advanced process nodes as the transistors are optimized for digital logic gates. Digital controllers on the other hand, thrive in a fast digital process as the controller bandwidth can simply be increased by increasing the operating frequency of the controller and have been demonstrated in [55, 50].

2.1.3 Low load efficiency management

Low load efficiency management is important to maintain a higher system energy efficiency during sleep states for the digital part. For PWM control, discontinuous conduction mode (DCM) is popular to improve low-load efficiency. The existing DCM controllers either use analog inductor current sensors or digitally sense the half bridge node in the power stage to detect negative inductor current. The on-time of the ground side transistor is adjusted to turn off the transistor precisely at zero inductor current [52]. Huang et. al. [52] achieves a precise DCM operation through an analog DCM calibration loop to improve robustness against variation. However the existing approach is not robust to variation in passives values as well as not suitable for integration in digital process nodes.

2.2 Side Channel Attacks and Countermeasures

Side channel attacks have been one of the most prominent threats to hardware and software implementations of encryption algorithms, which are secure against theoretical cryptanal-

ysis [14, 9, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 63]. Two of the most popular side channels exploited for attack are *power consumption*, where an adversary measures the supply current or power of the targeted system [30, 64] and *electromagnetic radiations* where the adversary measures EM signatures using a probe from the targeted system [10, 11, 65]. Countermeasures are design techniques that attempt to remove the correlation between the captured signatures and the internal switching activities. A successful SCA involves measuring the corresponding side channel for multiple encryption events, aligning the captured data with respect to the algorithm flow and performing statistical analysis on the data. Other than removing data-dependency in the captured signatures, another technique to thwart a SCA is to reduce the signal to noise ratio (SNR) of the captured signatures. The following subsections describe few major countermeasure categories widely used, particularly for AES engines.

2.2.1 Architecture/Algorithm based countermeasure

Table 2.1: Summary of Architecture/Algorithm based countermeasures

Countermeasure	**Platform**	**Area/Power Overhead**	**Performance Overhead**	**MTD**	**Year**
MUTE-AES [66]	Simulation	2x area 2x power	0.42%	No data	2008
Higher Order Masking [67]	FPGA	3x-4x area (order 1 to 3)	40x-160x (order 1-3)	No data	2010
Higher Order Masking on S-BOX [29]	8051 MC	2.5x-3x area	40-60%	240x	2011
Boolean Masking [68]	FPGA	2x-area	34%	No data	2012

An algorithmic or architecture based countermeasure tries to modify the internal computation steps of the encryption algorithm with maintaining functional correctness. An architecture-based countermeasure on the other hand, uses architectural techniques to re-

Table 2.2: Summary of selected logic style based countermeasures

Countermeasure	Platform	Area/Power Overhead	Performance Overhead	MTD	Year
WDDL [25]	ASIC	3x-area 4x power	4x	70x	2006
BCDL [69]	FPGA	4x-area	2x	>20x	2010
BBL [70]	ASIC	3x-area 0.7x-power	0%	720x	2015

duce the correlation between the power consumption and the internal steps of the algorithm. Table 2.1 lists some of the popular countermeasures in this category. One of the heavily used algorithmic countermeasure is masking [29, 68, 67] where the intermediate state is split in several partitions and are masked using random bytes. It is to be noted that these countermeasures, although effective in destroying the data-dependent switching current pattern, requires a careful redesign and verification of the logic.

2.2.2 Logic style based countermeasures

A logic style based countermeasure aims to generate a data independent switching power consumption from each logical operation. These countermeasures can be broadly classified into two categories. A set of proposed logic styles use completely new standard cells and requires a redesign of the synthesis library from scratch. Few examples of these countermeasures are Sense Amplifier Based Logic (SABL) [16], Dual Rail Random Logic (DRL) [71], three phase dual rail precharge logic (TPDL) [20] and bridge boost logic [70]. One of the key requirements for these techniques to successfully prevent a PSCA is balanced routing. A second category of logic style based countermeasure uses standard cells from a typical CMOS based library and achieves data independent power consumption from each logical operation. In wave dynamic differential logic (WDDL), a parallel combination of

Table 2.3: Summary of selected generic countermeasures

Countermeasure	Platform	Area/Power Overhead	Performance Overhead	MTD	Year
Shunt current equalization [15]	Simulation	2x power	0%	No data	2004
Switched Capacitor Current Equalizer [30]	ASIC	1.33x power 7% area	50%	>2500x	2009
Clock Randomization [73]	FPGA	1.1x	No data	>30x	2011
PDN Noise Injection [74]	FPGA	38% area 35% power	No data	>13x	2014

two complementary gates are used [25]. In Masked Dual-Rail Pre-charge Logic (MDPL) and improved MDPL (iMDPL), dual rail logic and masking are combined to improve robustness [72, 18]. The largest disadvantage with these countermeasures again is that area and power overhead increases significantly due to added computation to equalize the supply current.

2.2.3 Generic countermeasure

Both algorithmic and logic-style based countermeasures require a partial or complete redesign of the encryption engine, from HDL all the way to physical design and/or a completely new standard cell library. A generic countermeasure keeps the algorithm and the logic-style of the encryption engine intact. Other peripheral components like clock distribution and power delivery to the encryption engine are modified to alter the measurable signatures from the generated signatures. Shamir et. al. [14] first proposed the use of supply decoupling capacitance to attenuate side channel signatures in power measurement. A few of the important power-delivery based countermeasures include, injection of current noise [75] and switched-capacitor based current equalization [30]. One of the popular class of generic countermeasure is current equalizer circuits. Current equalization can be

achieved through a number of different methods.

1. A switched-capacitor based current equalization proposed in [30] uses a switched capacitor filter in series with the supply line. The encryption engine is powered by the local capacitors and it is ensured that the state of the capacitor before the charging phase is same for each cycle, which ensures the same charging current drawn from the supply.

2. A shunt current equalizer as proposed in [15] uses a series device in the power path to sense the supply current and equalizes it using a shunt loop.

3. Following a similar concept, a supply current attenuator is proposed in [76] and the authors also added a supply noise to further reduce the SNR of the measured signatures.

It is to be noted that these countermeasures are significantly lower in area and power overheads as well as require small design effort.

2.2.4 Voltage regulator based countermeasures:

With the advent of IVRs, the role of different IVR topologies on modifying side channel signatures have been studied recently as well.

LDO: A low dropout regulator dynamically adjusts the resistance of the pass device to regulate the output voltage at the local supply of the encryption engine. In a LDO, the local supply node is always connected to the input node through the pass transistor, which is always on, typically in saturation mode. Therefore the load signatures can easily propagate to the input signatures. The potential of a LDO in improving side channel resistance is attributed to the effect of the output capacitor as well as the small signal transfer function of the feedback path (error amplifier + output stage). Telandro et. al in [24] has shown that a LDO can reduce the peaks in the input current corresponding to a spiking load current pattern, which typically represents a generic digital block. However, no concluding

remarks on the improvement in side channel resistance is provided. Singh et. al. [40, 77] demonstrates the effectiveness of analog and digital LDO in improving side channel resistance. The authors mount a CPA and use measurement-to-disclose (MTD) as metrics for quantifying the side channel resistance. For analog LDO, the LDO bandwidth which is a function of the output capacitance value as well as the feedback loop gain, is used as a control knob for modulating side channel resistance. Digital LDOs have gained significant importance in recent years due to their ease of integration in advanced process nodes and avoiding issues with designing high bandwidth analog controllers at a digital process. For a digital LDO, the side channel resistance can be controlled by adjusting the ADC resolution, and the sampling speed of the feedback control.

Switched Capacitor: Yu et. al. in [78] proposed to use a multi-phase switched capacitor regulator for improving side channel resistance. Multiple phases for any switching regulator reduces the output ripple by interleaving the switching clocks for each phase. The authors used

1. Converter Gating: Depending on the total load current (includes the encryption engine and other digital blocks sharing the same supply rail) supplied by the IVR, the total number of active phases of the SC will change and the inactive phases will be gated

2. Converter Reshuffling: In a steady state condition the active phases of the SCVR are continuously reshuffled, changing the phase relationship between the input signature and the output signature.

The authors show that the gating and the reshuffling techniques successfully reduce the correlation ratio between the load power signatures and the input power signatures. Other than Pearson's correlation ratio, the authors also used power trace entropy to quantify the improvement in side channel resistance through the proposed methods.

Inductive Buck: The effect of fully integrated inductive IVRs on PSCA resistance

hasnt been studied before in the details, however, leakage at the input of an off-chip inductive VRM with low switching frequency ($\sim$100KHz) and high values of inductance and capacitance have been analyzed in [79]. The authors used a commercial off-the-shelf Texas Instruments Switcher with 300KHz switching frequency supplying a FPGA and analyzed leakage at the primary side of the switcher. Several post-processing techniques like wavelet based processing and deconvolution were used to successfully decode all 16 key bytes of an AES engine. However the observation suggests that the side channel resistance at the input side of a switcher is higher than the same at the AES supply node. Moreover an inductive IVR, due to its high switching frequency and loop bandwidth, will have enhanced mutual interaction with the information leakage from the underlying encryption engine, compared to the low frequency VRM used by the authors.

2.2.5 EM countermeasure

Rohatgi et. al. [12, 80] offer a comprehensive overview of EM side channel, signal post-processing steps as well as different attack methods. Some of the dedicated countermeasure techniques for preventing against EM attacks include e dynamic relocation of the data within a single encryption round as presented in [81] or use of duplicated complemented intermediate states as shown in [82]. Packaging and system level techniques like low-cost shielding as demonstrated in [83, 22] are also used for protection against EM leakage. However, these techniques are not scalable across platforms with different power ranges and often limited by packaging costs.

CHAPTER 3
MODELING AND ANALYSIS

IVRs are becoming an integral part of energy efficient digital systems due to smaller system footprint and improved transient performance, which can maximize benefits from DVFS. IVRs demonstrate fast recovery from voltage droops due to load current transients as well as fast switching from one reference voltage (corresponding to a power-state of the processor) to another reference voltage [41, 1, 42, 35, 43, 44]. VRs, specifically switching VRs like inductive buck regulators [55, 50] and SCVRs [42, 36] require passives (inductors and capacitors) which typically are implemented as discrete PCB components for VRMs with low switching frequencies. Over the years, integration of these passives within the silicon die or package has improved. New technologies for on-chip capacitance like trench capacitance have significantly improved the capacitance density, achieving up to 10nF/mm^2 than the traditional MOS caps (the capacitance of the gate oxide of the transistors) and MIM caps (Metal-Insulator-Metal). Similarly, technologies for on-chip inductors, on-package inductors and other forms of integrated inductance have matured over the last few years. However integrated passives are limited by the maximum achievable value, typically less than 10nH for inductances and 20nF for capacitances. This requires the switching regulators to use a higher switching frequency, typically more than 50MHz to limit the output ripple.

Existing IVR based PSCA resistance improvement schemes, as elaborated in section 2.2.4, exploits the isolation between the local supply of the encryption engine (output of the IVR) and the input of the IVR, as demonstrated in Fig. 3.1. When an IVR supplies power to a digital circuit, the only observable node to the adversary is the input of the IVR, as the local supply of the encryption engine is not connected to the package or the PCB. As power

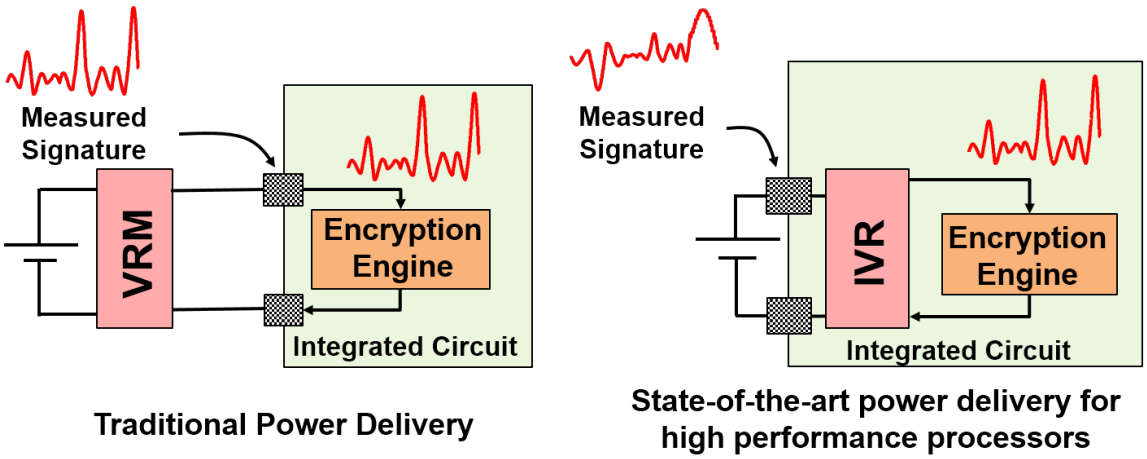

Figure 3.1: Effect of an IVR in transforming the generated side channel signatures from the measured signatures

measurements are invasive in nature, i.e. the adversary has to make physical contact with the target system, a side channel adversary can only measure power signatures at the IVR input. The load current signatures generated from the encryption engine are transformed through the IVR and the transformation depends on the nature of the IVR in context (LDO, SCVR, Inductive). Previous works have mostly focused on LDO based and SCVR based improvement in PSCA resistance [24, 77, 40, 84]. As it will be evident in the next few sections, the transformations through an inductive IVR are unique compared to a LDO or a SCVR. The input current drawn by an inductive IVR (the observed current at the supply pins) is a complex, frequency dependent transformation of the current consumed by the logic (Fig. 3.1). In the next few sections, the impact of the inductive IVR transformations on the power signatures of an encryption engine will be elaborated and the improvement in PSCA resistance will be quantified.

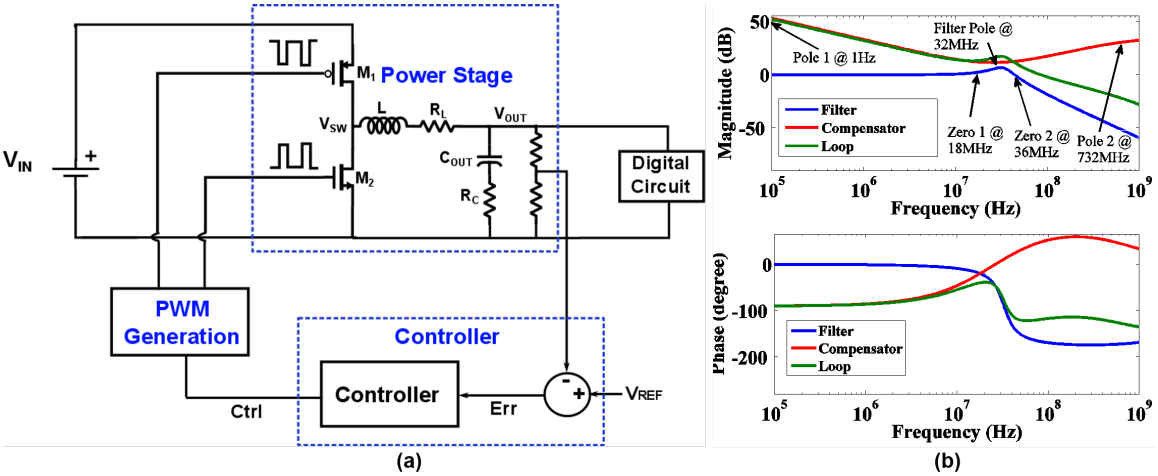

Figure 3.2: (a) Diagram of a generic inductive IVR (b) Bode plot of an illustrative IVR design with type III compensator

3.1 Fully Integrated Inductive Voltage Regulator

A generic inductive IVR has three major components: power stage, controller and PWM generator. The power stage consisting of switches M_1 and M_2 are driven by square waves. The switching node (V_{SW}) is filtered by the output filter consisting of a inductance and a capacitance. The filter pole created by the output passives ($1/2\pi\sqrt{LC}$) typically resides at 10MHz-50MHz (f_{LC}). To minimize output voltage ripple for lower passives, a higher switching frequency (F_{SW}) is used.

A voltage mode PWM controller compares the output voltage V_{OUT} to a reference voltage V_{REF}. As the phase across the output filter drops by 180° beyond the filter frequency, a compensator is needed to compensate the voltage error (ERR). The zero created by the ESR (R_C) of the output capacitor (C_{OUT}) and the capacitor itself resides at a high frequency ($1/(2\pi R_C C_{OUT})$) and does not add any phase lead, which is typical for an off-chip buck converter with higher passive values. Therefore, high frequency IVRs with integrated passives typically use type-III compensator. A type-III compensator places two zeros close to

f_{LC} and introduces a phase lead to compensate for the phase drop due to the double pole, as shown in Eqn 3.1.

$$G_C(s) = A\frac{(s+z_1)(s+z_2)}{(s+p_1)(s+p_2)} * e^{-st_d} \tag{3.1}$$

where z_1, z_2, p_2 and p_2 are the locations of the zeros and poles of the compensator respectively, A is the gain of the compensator, and t_d is the delay across the feedback loop, which represents the delay across the PWM generation as well as the switch drivers. A phase lag is added by t_d and can potentially make a control loop unstable. The following interesting points are to be noted from Fig. 3.2.

- The filter frequency of an IVR lies close to the loop bandwidth or the unity gain frequency (UGF), making the IVR loop characteristics sensitive to the location of the filter pole.
- For analog controller, a typical value of t_d is 400ps-600ps and does not scale with the switching frequency, whereas for a digital controller, t_d depends on the steady state duty cycle. As the value of t_d is comparable to the switching period for a high frequency VR, the sensitivity of the IVR loop to t_d is higher than their off-chip counterparts

A PWM generator converts the compensated error value to a square wave with appropriate duty cycle and drives the transistors M_1 and M_2. An analog PWM generator uses a sawtooth-comparator combination to convert the compensated error into a square wave with duty cycle. A digital PWM generator takes a digitized word representing the compensated error and uses different primitives like counters or delay locked loops to generate a square wave with duty cycle.

3.2 Transformations of an Inductive IVR

Understanding the effectiveness of an inductive IVR in improving PSCA resistance of an encryption engine requires analysis of the transformations of the current signatures from

the output node of the IVR to the supply of the IVR. These transformations are dictated by the IVR's switching frequency, the values of the IVR's passives as well as the IVR controller structure.

Large Signal Transformation

In a steady state operation i.e. a steady load current and reference voltage, the power stage of the IVR continuously switches i.e. the transistors M_1 and M_2 periodically turn on and turn off (Fig. 3.3). When M_1 in on, the input current (I_{IN}) is equal to I_L and when M_2 in on, I_{IN} drops to zero. The continuous switching of the power stage creates a pulsating pattern at the IVR input current, irrespective of whether the underlying digital logic supplied by the IVR is active or not. Each silicon die is accompanied with a package which connects the die pads to the external PCB. The package connections offer parasitic inductance (L_{PKG}) and resistance (R_{PKG}) and an on-chip decoupling capacitance (C_{DECAP}) at the IVR input is needed to compensate for the ringing caused by the package parasitics. The sharp change in I_{IN} when M_1 turns off introduces $\frac{\partial i}{\partial t}$ ringing due to the package parasitics and modifies I_{IN}. A lumped model of the package parasitics is used later to model this effect. With advanced packaging techniques like C4 bumps, the effect of package parasitics is less significant on the large signal transformation. Wang et al. [74] have shown that the package can play an important role in improving PSCA resistance. However the parasitics values assumed by the authors are significantly higher than advanced packaging techniques like C4 bumps.

One of the most effective contribution of the large signal transformation is hiding the location of the encryption events in the recorded traces. For a practical PSCA, the adversary might not have access to the internal trigger signal which denotes the start of the encryption operation. In the absence of an on-chip VR, the starting of the encryption event can easily be found out by observing the change in supply current. However the switching current at the IVR input is significantly higher in magnitude than the current of the encryption engine and is effective in hiding the current signature.

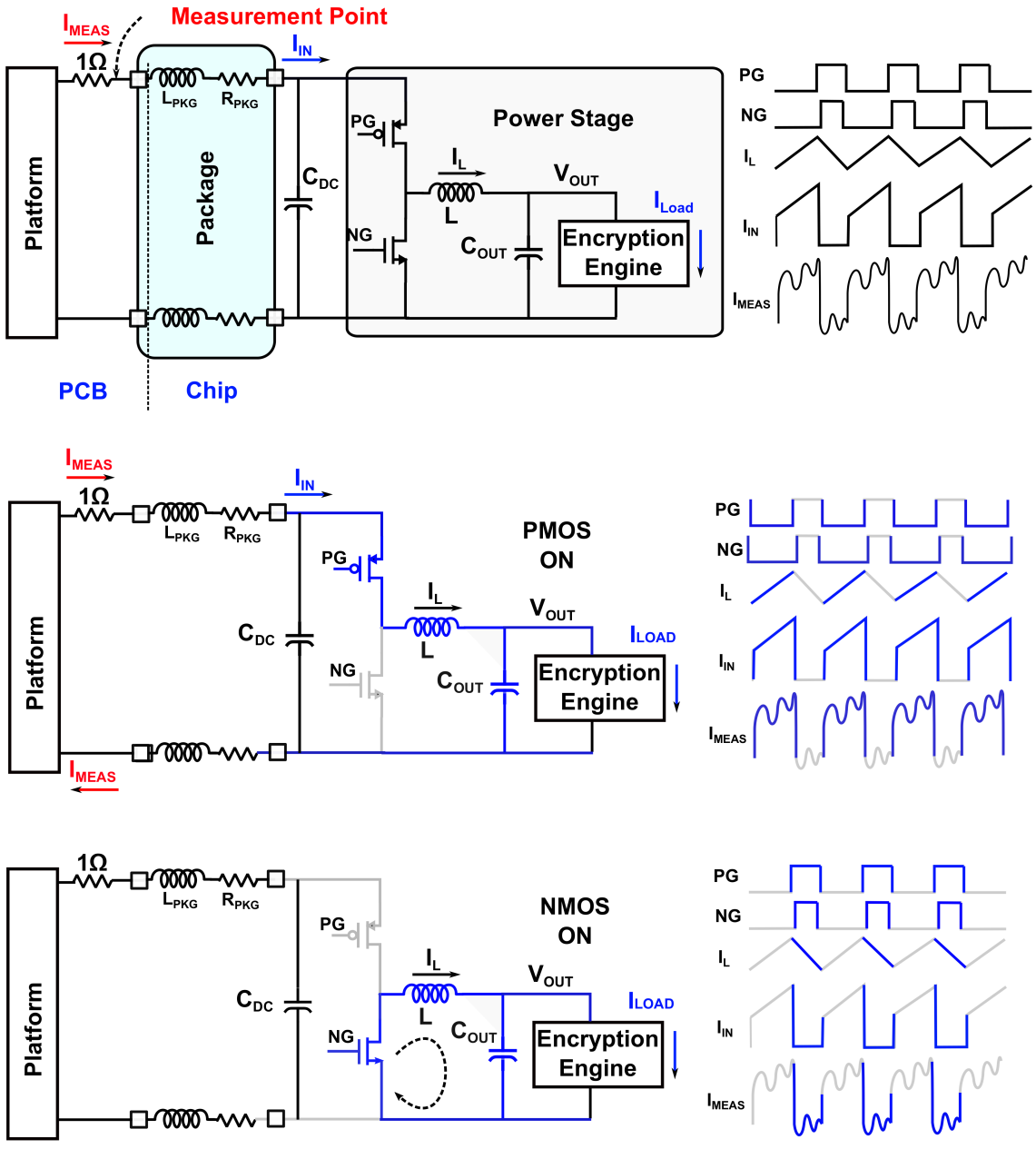

Figure 3.3: Large signal transformation

Small Signal Transformation

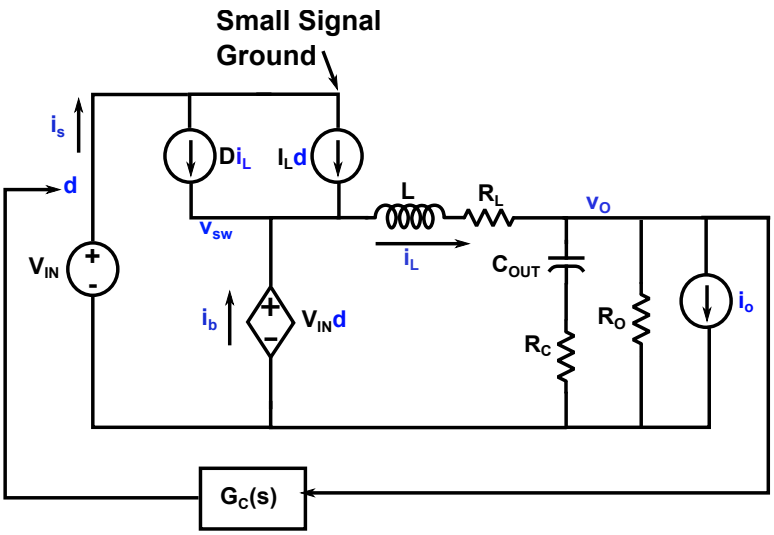

Figure 3.4: Small signal representation of the control loop of an inductive IVR

Fig 3.4 shows the small signal representation of an inductive IVR. It is assumed that the V_{REF} as well as the input voltage V_{IN} remains fixed (equivalent to ground in the small signal representation) and the control loop is simplified accordingly. The input current of the IVR can be expressed by the following equation:

$$i_{in} = i_l * D + d * I_L \tag{3.2}$$

where i_{in}, i_l and d are small signal input current, inductor current and duty cycle respectively. I_L and D are steady state average values of the inductor current and the duty cycle respectively. I_L can also be approximated as I_O or the average load current supplied by the IVR. The small signal component of the input current, as dictated by Eqn 3.2, consists of two components, each of which represent a small signal path leakage path. When M_1 is on, i_{in} can be approximated as i_o which is the small signal load current signature. Therefore turn on time of the M_1 acts as a window through which the load current signatures leaks from IVR output node to IVR input node, representing the first term in Eqn 3.2. This is small signal leakage through the IVR power stage. The duty cycle of the square waves

generated by the compensator represents another small signal path for leakage. This is represented by the second term in Eqn 3.2. The current signature of the IVR load (encryption engine) generates voltage signature at V_{OUT} node due to non-zero impedance looking into the IVR. The voltage signature propagates through the control path and is modified by the compensator transfer function. The coefficients of the compensator determine the locations of compensator zeros and poles, which dictates the compensator transfer function.

3.3 Simulation Details

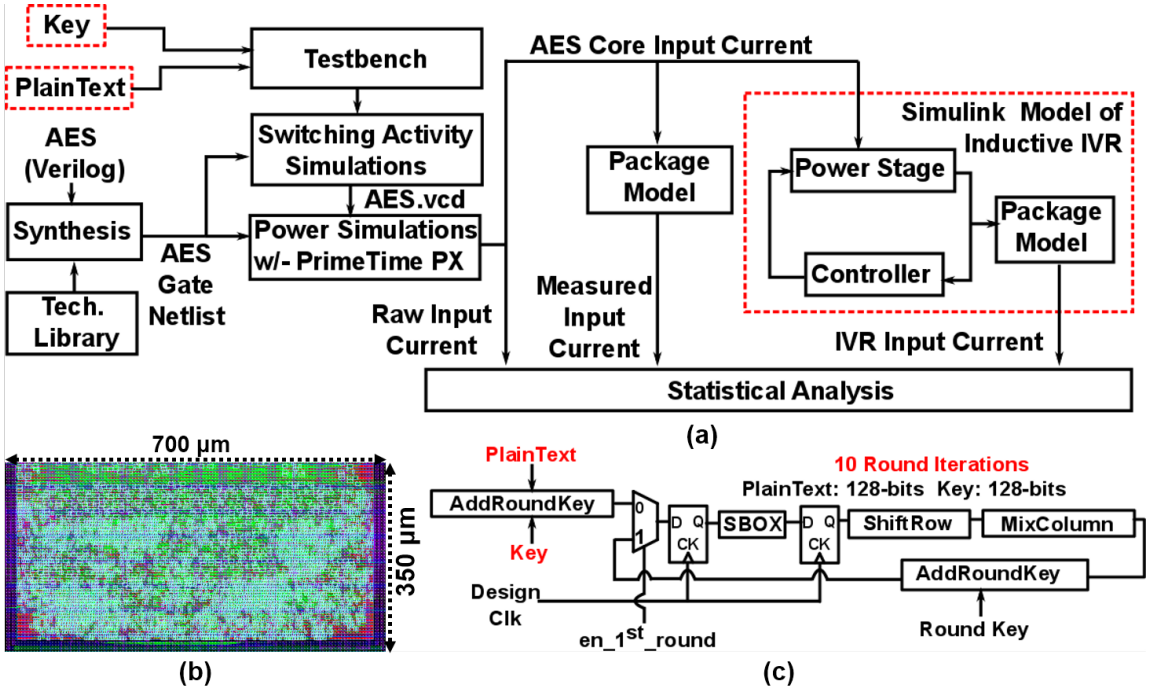

Figure 3.5: (a) Simulation framework for the analysis (b) Physical design of the AES engine (c) Architecture of the AES engine

To understand the impact of these transformations, a 128-bit Advanced Encryption Engine (AES) is used as the baseline encryption engine. The simulation infrastructure is shown in Fig. 3.5. A 128-bit AES engine accepts a 128-bit plain-text and a 128-bit key and generates a 128-bit cipher-text. The AES architecture, used for the simulation framework

is shown in Fig. 3.5c. Each AES encryption consists of 10 rounds, each round except the last round, consisting of four steps: substitution box (SBOX), Shiftrow, MixColumn and round key addition (Addroundkey). The chosen architecture uses a two stage pipeline; the first stage consisting of only SBOX, which typically exhibits the longest datapath and the second stage consisting of the rest of the operations. The rounds are executed serially in the implemented architecture with a 128-bit datapath, i.e., all bytes of the 128-bit intermediate state are processed in parallel. One AES encryption takes 20 clock cycles. The verilog of the AES is synthesized using a 130nm standard cell library at 1.2V supply voltage and the corresponding physical design after place and route is shown in Fig 3.5b. The maximum frequency of operation (F_{MAX}) after place and route was found to be 125MHz. A testbench is used to simulate the gate level netlist with one key and multiple plaintexts. Synopsys Modelsim is used for gate level simulations of the synthesized AES netlist and Synopsys PrimeTime (PT) is used to generate the power traces from switching activity files (.vcd) corresponding to each encryption run.

A Simulink based time-domain model of an inductive IVR, adapted from [85], is used to generate the IVR input current traces from a load current PWL signal. The parasitic model of a C4 package is also used in the time-domain simulation. Both the raw AES current trace, the AES current measured after package and the current at the IVRs input are used for further statistical analysis.

3.4 Correlation Study with An AES Engine

Correlation Transfer Function

Pearson's correlation coefficient is a statistical metric that quantifies the similarity between two matrices.

$$r_{xy} = \frac{\sum_{n=1}^{n}(x_i - \overline{x}) \sum_{n=1}^{n}(y_i - \overline{y})}{\sqrt{\sum_{n=1}^{n}(x_i - \overline{x})^2 \sum_{n=1}^{n}(y_i - \overline{y})^2}} \tag{3.3}$$

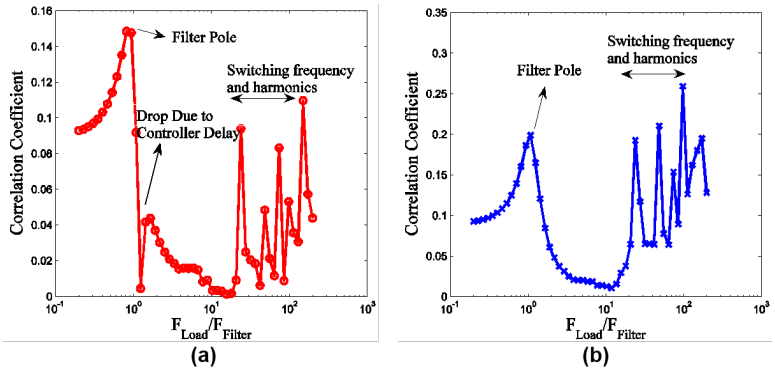

Figure 3.6: Correlation between for a sinusoidal load current with varying frequency and the corresponding IVR input current in (a) time domain and (b) frequency domain

The correlation between the IVR load current signature and the input current signature can be used to quantify the effect of both small-signal and large-signal transformation. A correlation transfer function (CTF) is constructed by computing correlation between a sinusoidal load current and the corresponding IVR input current for varying frequency of the sinusoid (F_{LOAD}). The correlation value is plotted against the ratio of F_{LOAD} to the filter frequency (F_{FILTER}, 5MHz for an illustrative IVR design) in Fig. 3.6a. Fig. 3.6b shows the correlation between FFT of the load current and FFT of the input current. Both in time and frequency domain the correlation peaks near F_{FILTER}. With increasing F_{LOAD} the closed loop gain of the IVR drops beyond the loop bandwidth, therefore, decreasing the gain from the output current to input current. Hence, the correlation starts dropping after F_{FILTER}. However, in the time domain correlation, inconsistent trends (the correlation drops abruptly at certain frequencies) are observed. This effect is due to the delay in the controller path that introduce variable phase shifts with varying F_{LOAD}. The phase shift is contributed by the fixed delay in the control path (due to computation) as well as phase shift introduced by the compensator. If the total phase shift is close to 90° or 270°, correlation value in the time domain can drop significantly. The peaks in correlation near F_{SW} and its harmonics are due to the switching of the IVR.

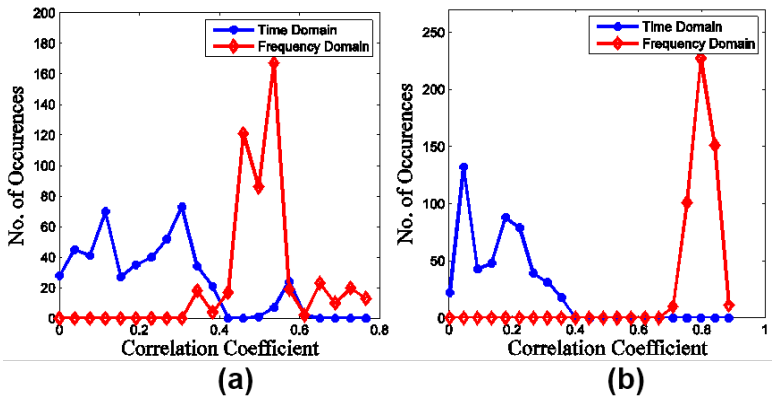

Figure 3.7: Distribution of correlation coefficient for different post-processing techniques applied to the IVR input current in time and frequency domain. (a) envelope and (b) duty cycle

Correlation With AES Load Current Traces

A set of 500 power traces generated from the AES engine, for 500 plain-texts and a single key, are considered for a correlation study. Two post-processing techniques are applied on the IVR input current to understand the impact on the correlation values; envelope and duty-cycle and the mean correlation is observed to improve. Fig 3.7 shows the distribution of the correlation coefficient (for 500 power traces) in time and frequency domain for these two techniques. Interestingly, along with a higher mean, the frequency domain analysis also lowers the spread compared to the time domain. The reduced mean in the time-domain analysis is attributed to the phase shift in the control loop. As each load trace has different frequency spectrum, the phase shift through the compensator is different for various traces creating significant variation in correlation coefficient in the time-domain analysis.

The above analysis was published in [86]. It shows that IVR transformations reduce the correlation between the load current signature and the input current signatures, significantly. Although post-processing in the frequency domain or computing the envelope and duty-cycle, improve the absolute values of correlation, a lower correlation value does not guarantee improved resistance against a key-extraction attack like a CPA. In the next

section, it will be demonstrated that the IVR input signatures are vulnerable to an actual key-extraction attack in both time and frequency domain, without the need for any post-processing techniques.

3.5 Power Attack on IVR-AES

In a traditional key-extraction attack like CPA, even if the absolute magnitude of the correlation for each key guesses is very small ($\sim$0.01), it suffices if the correlation of the correct key-guess is higher and distinguishable than the correlation of the incorrect key guesses. Although correlation does provide an idea about how difficult it would be to mount a successful PSCA, mounting an actual key-extraction attack is necessary to quantify the resistance against PSCA.

3.5.1 Modeling of IVR

The correlation study presented in the last section is performed on an illustrative IVR with 20nH inductance, 50nF capacitance (f_{LC} 5MHz). The small signal transfer function from load current to input current, as well as the CTF, show that the correlation between the load current and the input current attenuates beyond IVR loop bandwidth. As an AES engine typically operates at a much higher frequency, the small signal attenuation offered by the illustrative IVR with 20nH inductance and 50nF capacitance is expected to be higher at the frequencies of interest (at and beyond the AES clock frequency) and show better PCSA resistance. For the following analysis, the inductance and capacitance values are reduced and the switching frequency is increased to create a vulnerable IVR design where the attenuation of the load signatures at the IVR input near the frequencies of interest is lower. The IVR power stage uses 4nH inductance and 6nF capacitance, with 400MHz F_{SW}. An analog type III compensator with the following pole-zero locations are used for the

time-domain simulation of the IVR.

$$\begin{aligned} p_1 = 1 \quad p_2 = 2f_0\sqrt{\frac{1+\sin\theta}{1-\sin\theta}} \\ z_2 = 2f_0\sqrt{\frac{1-\sin\theta}{1+\sin\theta}} \quad z_1 = 0.5 * z_2 \\ f_{LC} = \frac{1}{2\pi\sqrt{LC_{OUT}}} \quad f_0 = 5f_{LC} \end{aligned} \tag{3.4}$$

Table 3.1: Details of the illustrative IVR for power-attack study

F_{SW}	L	C_{OUT}	f_{LC}	ϕ_M	UGF	p_1	p_2	z_1	z_2
400MHz	4nH	6nF	32.4MHz	61	83MHz	1Hz	732MHz	18MHz	36MHz

3.5.2 CPA and Power-Model

CPA is chosen to quantify the effectiveness of inductive IVR in improving PSCA resistance. CPA is a byte-wise attack which exploits a particular intermediate step of the AES where the computation depends on one byte of the key and one byte of the state. In CPA a set of known plain-texts are encrypted with an unknown key and powermodels are constructed for all possible key-guesses for all 16 bytes of the key (16 powermodels). Pearson's correlation coefficient is calculated between the columns of measured power traces ($[M]_{P\times T}$, T: length of recorded trace for one encryption assuming a fixed sampling rate, P: total number of encryption events measured) and power-model ($[HD]_{P\times K}$, K: all possible guesses of the attacked key byte).

The AES netlist is synthesized in 130nm IBM-8RF standard cells with a 125MHz clock. For the following results, the hamming distance at the SBOX output of the first round is used as powermodel. The powermodel captures the power consumption of the SBOX output register shown in Fig. 3.5c, in particular the 8 flipflops associated with the corresponding key-byte. The highest value of correlation coefficient $\rho(t,k), 1 \leq t \leq T, 1 \leq k \leq K$

identifies the correct key (k').

3.5.3 Example Waveforms

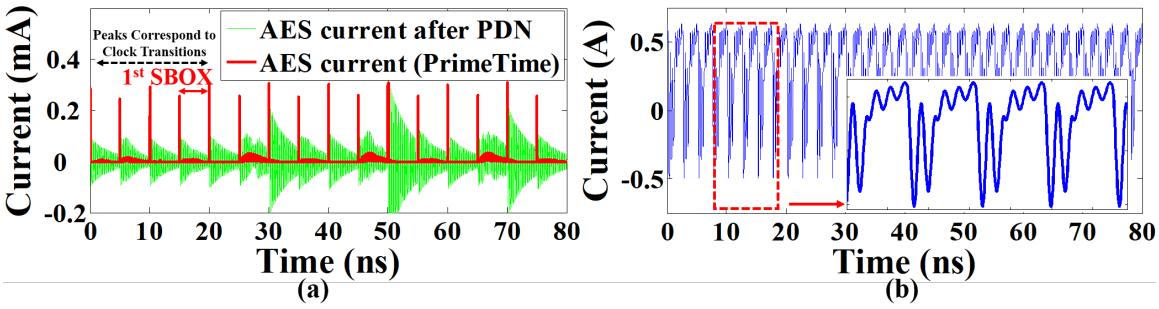

Figure 3.8: Simulated current signatures (a) AES encryption current before and after PDN (b) Measured current at the input of an IVR

Fig. 3.8a shows the input current corresponding to one encryption run of the designed AES engine, before and after the PDN. Fig. 3.8b shows the corresponding time-domain current pattern at the supply pins of the IVR. Due to extremely small magnitude of the current variation of the AES engine, there is almost no visual variation in the input current of the IVR. The zoomed version (given in inset) shows that the input current has a pulsating pattern at the switching frequency of the IVR (F_{SW}) along with ringing introduced by the package.

3.5.4 CPA on AES Engine

To characterize and quantify the vulnerability of a design, the following metrics are used

- CPA status (successful or unsuccessful)
- MTD (if a successful CPA happens)
- Correlation ratio (the ratio of maximum correlation value across the entire trace length of the correct key to the maximum value across all the other incorrect keys)

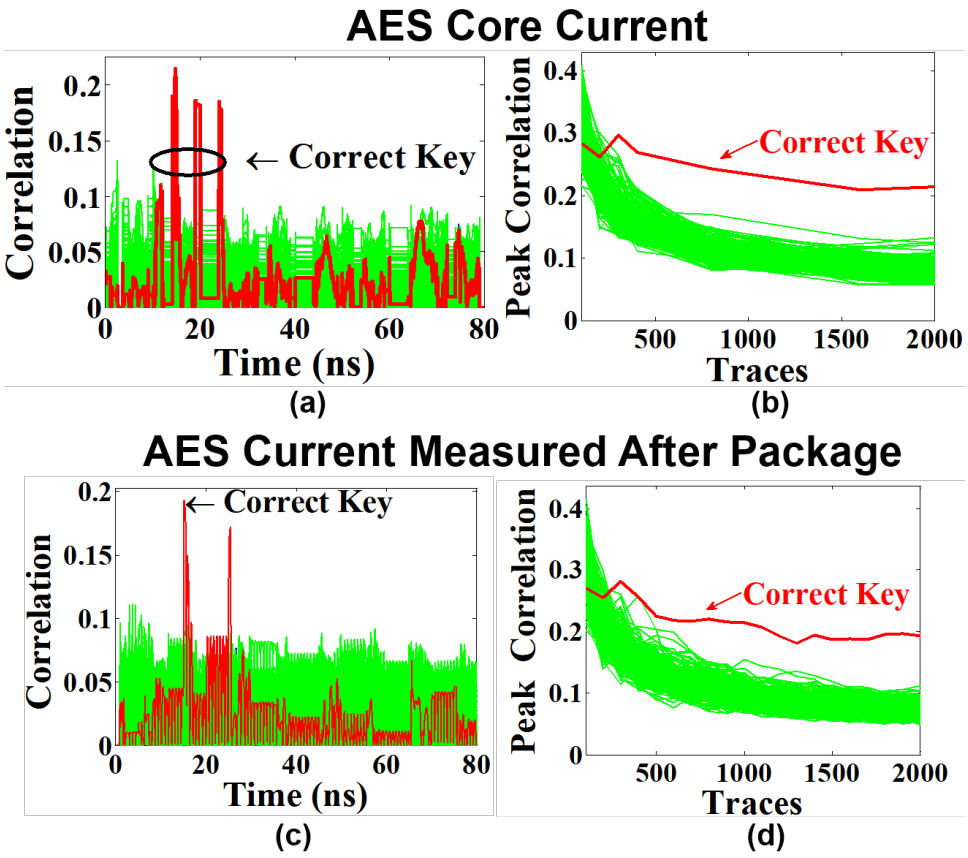

Figure 3.9: CPA on the standalone AES engine (red: correct key, green: 255 incorrect keys) : (a) Correlation coefficient against time for the correct and incorrect keys for AES core current (b) MTD plot of the AES core current. Peak correlation vs number of traces for 250, 500, 1000, 2000 traces is shown. (c) Correlation coefficient with the effect of package parasitics for the correct and incorrect keys (d) MTD plot of AES current measured after package

The correlation ratio is an indicator of how easy it will be to perform a successful CPA in presence of measurement noise (not accounted for in this work). Fig. 3.9a shows the correlation coefficients versus time for 256 possible guesses for the 1st key byte on the AES supply current. The correlation for the correct key byte (red curve) shows distinct peaks from 15ns to 25ns. A successful CPA is observed if the number of traces is more than 250 (i.e. MTD = 250, Fig. 3.9b). Another experiment models the package and the PDN in the power delivery path to the AES engine with the following parameters: L_{PKG}=25pH, R_{PKG}=25mΩ, C_{DECAP}=100pF). The CPA on measured AES current in such systems showed similar attack resistance (MTD = 250) as the standalone AES core (Fig. 3.9c,d). The study indicates that the transformation induced by the package does not affect the power attack resistance. For the rest of the analysis, the Simulink model considers the effect of a package and an on-chip PDN.

3.5.5 CPA on the illustrative IVR-AES system

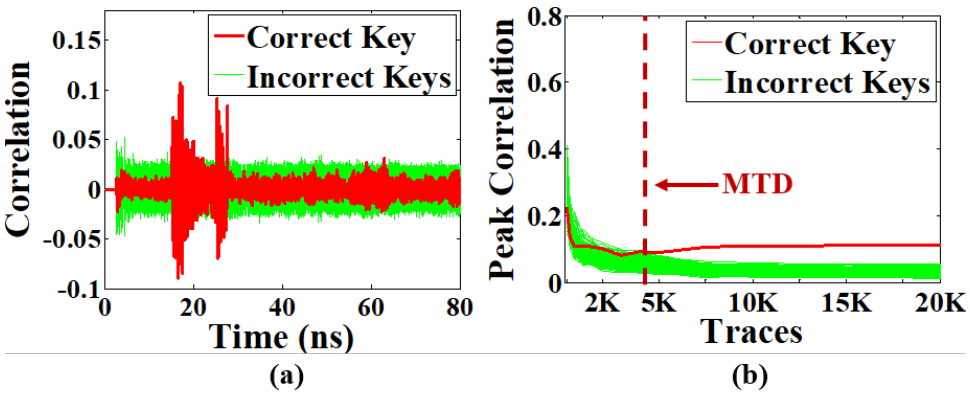

Figure 3.10: (a) CPA results on the input current of the illustrative IVR design (b) MTD plot of the illustrative IVR-AES system

The illustrative IVR is designed with the parameters shown in table 3.1 and the compensator model shown in Eqn 3.4. Following the simulation methodology described in section 3.3, the corresponding currents at the IVR input are generated and a CPA is performed on

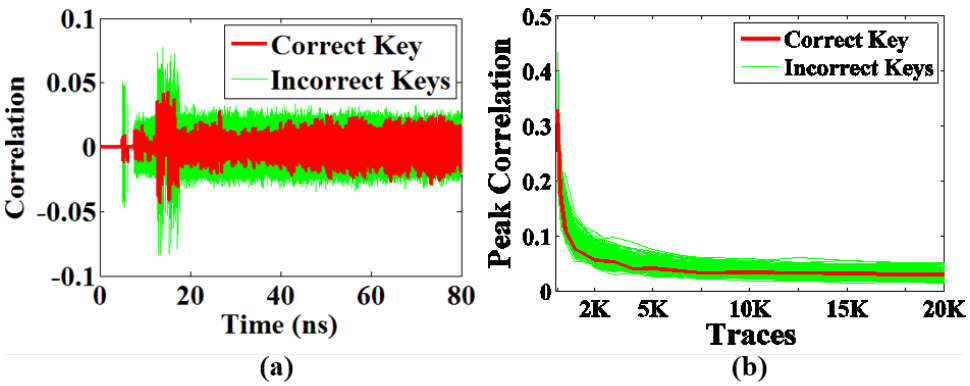

Figure 3.11: (a) CPA results on the input current of an IVR design with feedback loop delay. An example design with t_D=1ns is shown. (b) MTD plot of the AES-IVR system with t_D=1ns

the IVRs input current. A successful CPA is observed at the IVR input for the illustrative design (Fig. 3.10a). The MTD of the IVR-AES system is found to be 4000 (Fig. 3.10b). The MTD increased by 16x compared to the baseline design. Although the absolute value of the correlation for the correct key has decreased in an IVR-AES system, the correlation ratio remains high, indicating that calculating absolute correlation value [86] is not enough to ensure attack protection. Therefore, it is important to consider security-aware design strategies to improve robustness.

3.6 Security Aware Design Strategies for IVR

$$L_G(s) = G_{VD}(s) \times G_C(s) \tag{3.5}$$

The improvement in attack resistance for IVR (for eg. 16x increase in MTD for the baseline IVR) is attributed to the small signal and large signal transformation from the load current to the input current. A security aware IVR design aims at modifying these transformations to increase attack resistance. The large signal transformation is determined by the switching frequency of the IVR which is often fixed by the target power efficiency of the IVR and in some cases EMI constraints. Small signal transformation on the other

hand is solely determined by the small signal loop characteristics (expressed in Eqn 3.5; $G_{VD}(s)$ is control to output transfer function and $G_C(s)$ is defined before). Any change in the magnitude and the phase of $L_G(s)$ would change the small signal transformation and would eventually alter the attack resistance.

$G_{VD}(s)$ can be changed through changing passive values (L and C) and their corresponding parasitics (R_L and R_C). Increasing the values of L and C helps in improving attack robustness; for eg. an IVR with L=5nH, C=10nF and F_{SW}=300MHz shows an unsuccessful CPA. However, in most of the commercial designs, L and C values are fixed by different performance metrics such as maximum inductor current ripple, loss across R_L and worst case droop as well as the achievable passive density in the corresponding technology node. The current trend in IVR design is to use low passives that can be embedded even in small dies.

$G_C(s)$ on the other hand can be modulated by control topologies and circuits, and is not limited by process (or packaging) constraints. Moreover $G_C(s)$ can also be modified on-the-fly as long as the IVR output is stable. Therefore, security-aware IVR design strategies need to focus on modulating $G_C(s)$ for power attack protection. However, modulating $G_C(s)$ also affects a number of performance metrics namely transient droops and settling time, and hence, understanding the trade-off between security and performance is crucial. $G_C(s)$ is modulated through changing θ (in general pole-zero locations) and t_D (loop delay) in Eqn. 3.4. Other parameters like controller gain (A in Eqn. 3.4) can also be used to modify $G_C(s)$. F_{SW}, L, and C values are not modified from the baseline design.

3.6.1 Effect of controller delay

A nonzero controller delay introduces additional phase lag in the loop, reducing the loop phase margin (PM), but the magnitude response remains unchanged. Additional loop delay significantly improves the attack resistance as shown in Fig. 3.12. 0.5ns extra delay in the loop increases the MTD by 3.75x compared to the baseline design, whereas 1ns delay

Table I: Security Aware FIVR Design: Controller Delay L=4nH, C=6nF, F_{SW}=400MHz, θ=65°							
Controller Delay (nS)	Attack Parameters of FIVR Input Current			Performance Metrics of FIVR			
	CPA	*MTD	*Ratio	UGF (MHz)	Phase Margin (°)	Settling Time (nS)	Droop (mV)
0	Successful	4000	2.60	83.0	61.1	25.1	80
0.5	Successful	15000	1.22	83.0	55.7	27.3	196
1	Un-Successful	N/A	0.78	83.0	43.2	32.4	250

Figure 3.12: Effect of controller delay on PSCA improvement

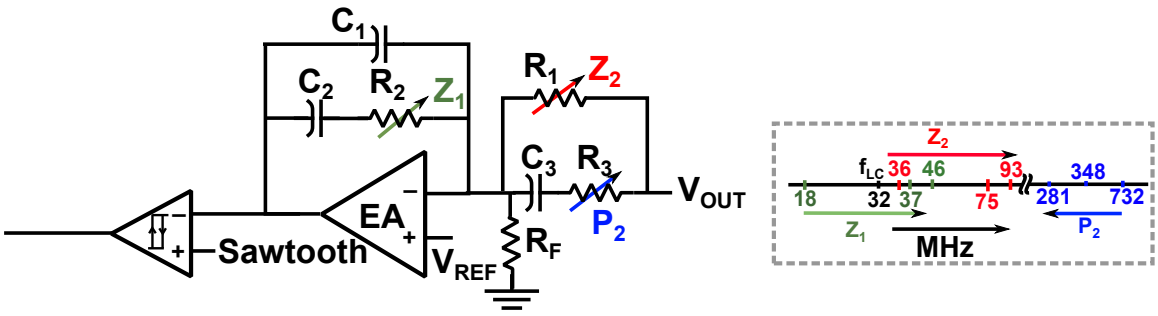

Figure 3.13: Movement of poles and zeros in the IVR compensator for decreasing and implementation of security-aware IVR design techniques.

makes the design robust from a CPA (Fig.3.11). The correlation ratio also decreases in coherence with the improvement in MTD. This clearly shows that controller delay can be used to improve PSCA resistance (Fig. 3.12). The improvement comes at the cost of low phase-margin of the system that increases the droop and settling time for a sharp load transient. The worst case phase margin is 43.2° (at 1ns delay) which is still more than the 40° phase margin of IVR in Haswell [41]. For implementation purposes, additional delay can be achieved by using a programmable delay generator after the PWM (analog control) or the DPWM (digital control) output, as shown in Fig. 3.13.

Table II: Security Aware FIVR Design: Compensator Transfer Function L=4nH, C=6nF, F_{SW}=400MHz, t_D=0							
θ (°)	Attack Parameters of FIVR Input Current			Performance Metrics of FIVR			
	CPA	*MTD	*Ratio	UGF (MHz)	Phase Margin (°)	Settling Time (nS)	Droop (mV)
65	Successful	4000	2.60	83.0	61.1	25.1	80
40	Successful	10000	1.62	150.5	33.5	27	72
30	Un-Successful	N/A	0.58	174.1	21.9	30	72

Figure 3.14: Effect of compensator transfer function on PSCA improvement

3.6.2 Effect of compensator transfer function

Changing compensator pole zero locations (parameter θ in 3.4 for the present setup) changes the compensator transfer function. When θ is changed from 60° to 45° and 30°, the bandwidth of the loop increases whereas the phase margin decreases. The pole zero movements in the design are shown in Fig. 3.13. From the context of power attack protection, reducing θ also improves the attack resistance significantly (Fig. 3.14), but at the expense of reduced phase margin (higher settling time). As the AES engine by itself does not generate any sharp load transients, the security aware compensator modes (either controller delay or pole-zero) during an AES operation do not show any significant change in the output voltage, even in the presence of clock transition spikes and reduced PM of the IVR. For an analog controller, pole zero can be changed dynamically by using tunable resistor and capacitor arrays in the compensator (Fig. 3.13). For a digital controller, this amounts to change in the digital coefficients of the PID filter.

3.7 Alternative Attack Modalities

The transformations described in section 3.2 can broadly be described as linear transformations which spreads out the information contained in the load current signatures into multiple cycles of the IVR input phases. Traditional attack modalities like time domain

CPA might not be efficient to prove or disprove the effectiveness of the IVR. In this section, alternate attack modalities which are more robust against linear transformation or time-shift based countermeasures, are explored.

3.7.1 Frequency Domain Analysis

The underlying assumption behind statistical tests performed to analyze side channel leakage is that at a given sample point of all or most of the recorded traces, the same step of the algorithm is executed. However, as explained in section 3.2, the mapping of load current signatures of a particular round to the corresponding IVR input current is one-to-many. The magnitude of the Fourier Transform of a trace is independent of the phase (time-shift) and can be used to perform a CPA. FFT of a signal can be represented as

$$FFT(M_{i,1:T}) = \sum_{n=0}^{T-1} M_{i,n+1} \times W^{nm}, W = e^{-j\frac{2\pi}{T}} \tag{3.6}$$

As the FFT magnitude is an even function of frequency, only one half of FFT output is used to constitute a matrix $[FM]_{P\times T/2}$. In frequency domain attacks, same power model as time domain attack can be used; as amplitude in frequency domain is proportional to amplitude in time domain, irrespective of the time shift. Next the correlation between HD and FM is computed.

$$\rho_{FFT}(j,k) = corr(FM_{1:P,j}, HD_{1:P,k}) 1 \leq j \leq T/2, 1 \leq k \leq K \tag{3.7}$$

A major challenge in frequency domain CPA is that the FFT cannot capture the data dependent activities with sufficient resolution, as the exploitable signatures (the part of the signature that corresponds to the power model) occur over very short time duration. For a sufficiently large recorded trace, activities might not be visible in the frequency domain. A small window can be used to compute the FFT, however, it can limit the effectiveness of frequency domain analysis if the worst case time-shift is outside that window. To counter

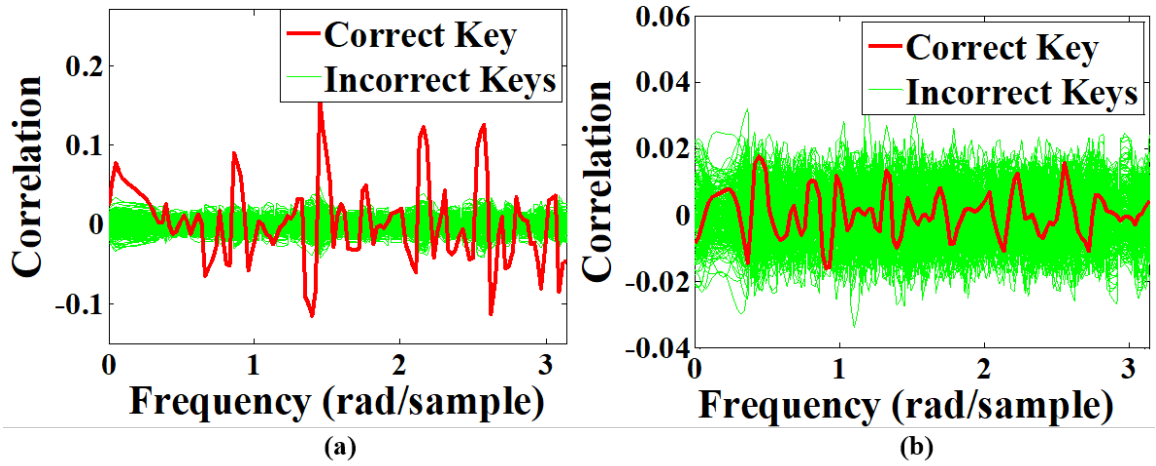

Figure 3.15: CPA in frequency domain (Spectrogram) for two IVR designs (a) Baseline IVR (b) IVR design with θ=30°. The correlation is plotted against a normalized frequency vector from 0 to π.

this, short-time Fourier transform (STFT) is used to observe the spectral content over time. Spectrogram, which is the squared magnitude of STFT of the power traces can also be used for performing CPA. Time-localized frequency content of a spectrogram is plotted against normalized frequency.

Results

A Hamming window of 128 samples (F_{SAMP}=10ps) is used for calculating spectrogram in MATLAB and replace the matrix FM (Eqn 3.7) with the spectrogram coefficients (dimension of FM is now $P \times W$ where w is the length of a vector of normalized frequencies) for correlation calculation. Fig. 3.15 shows the attack on spectrogram on the baseline IVR design (=65°) and a design with different controller pole-zero locations (=30°). The security-aware IVR designs also improve the attack robustness in frequency domain CPA; a design that is protected (un-protected) in the time-domain is also protected (un-protected) in the frequency domain.

3.7.2 Threat Model

A potential attack modality on the IVR input current is to reverse-engineer the transformation through the IVR by using an inverse transformation and recover the AES current signatures from the measured IVR input current signatures. Accurately extracting the transfer function is highly challenging; however, under a pessimistic scenario where an adversary can accurately reconstruct the transfer function, it is important to understand whether the improvement in PSCA resistance at the IVR input can be nullified.

The large signal distortion, introduced by the switching frequency of the IVR, can be filtered out from the IVR input current through a simple low-pass or a band-pass filter. However, as explained in Fig. 3.3, the on-time of the transistor M_1 during every switching period acts as a window where the load current signature directly appears at the IVR input. This effect cannot be reversed through filtering out F_{SW} component at the IVR input current. The small signal transformation from load current to input current can be modeled, and the adversary can use an inverse transfer function to estimate the load current from measured input current, as discussed next.

Current Transformation through an IVR

The small signal representation of the input current of the IVR has been shown in Eqn3.8. The equation can be rewritten as

$$i_{in} = (D\frac{i_l}{v_o} + I_0\frac{d}{v_o}) \times v_o = (D\frac{i_l}{v_o} + I_0\frac{d}{v_o}) \times \frac{v_o}{i_o} \times i_o \tag{3.8}$$

The small signal duty cycle (d) to voltage (v_o) gain can be written as

$$\frac{d}{v_o} = -G_C \times M \tag{3.9}$$

where G_C is the compensator transfer function, including the small signal gain across ADC and DPWM and M is the gain across the power stage. The small signal inductor current (i_l) to voltage (v_o) gain can be written as

$$\frac{i_l}{v_o} = -\frac{1}{Z_1} \times (1 + G_C M V_{IN}) \tag{3.10}$$

Finally the closed loop output impedance i.e. $\frac{v_o}{i_o}$ can be represented as

$$\frac{v_o}{i_o} = \frac{1}{\frac{1}{Z_2} + \frac{1}{Z_1}(1 + G_C M V_{IN})} \tag{3.11}$$

where $Z_2 = (1/sC_{OUT} + R_C)||R_O$ and $Z_1 = sL + R_L$ The magnitude of the transfer function (Eqn 3.8) at very low frequency is equal to the duty cycle D (V_{OUT}/V_{IN}). At higher frequencies the magnitude peaks near the resonant frequency of the output filter and eventually drops, governed by the loop-bandwidth. This clearly suggests that the high frequency load current components are heavily attenuated and never appear at the input current.

Reversibility

The reversibility transfer function (RTF) from the IVR input current to the load current is the inverse transfer function of Eqn 3.8 and is expressed as:

$$RTF = \frac{i_o}{i_i n} = \frac{\frac{1}{Z_2} + \frac{1}{Z_1}(1 + G_C M V_{IN})}{\frac{D}{Z_1}(1 + G_C M V_{IN}) + I_O G_C M} \tag{3.12}$$

The magnitude and phase of RTF are plotted in Fig. 3.16a for the baseline IVR. The low frequency gain is equal to 1.5 which is also equal to the inverse of steady state duty cycle (1/D=1.8/1.2). The gain drops near the filter frequency ($1/2\pi\sqrt{LC} = 32.4MHz$). The RTF gain increases after the filter cutoff frequency to compensate for the attenuation at high frequency in the forward transfer function ($\frac{i_{in}}{i_o}$).

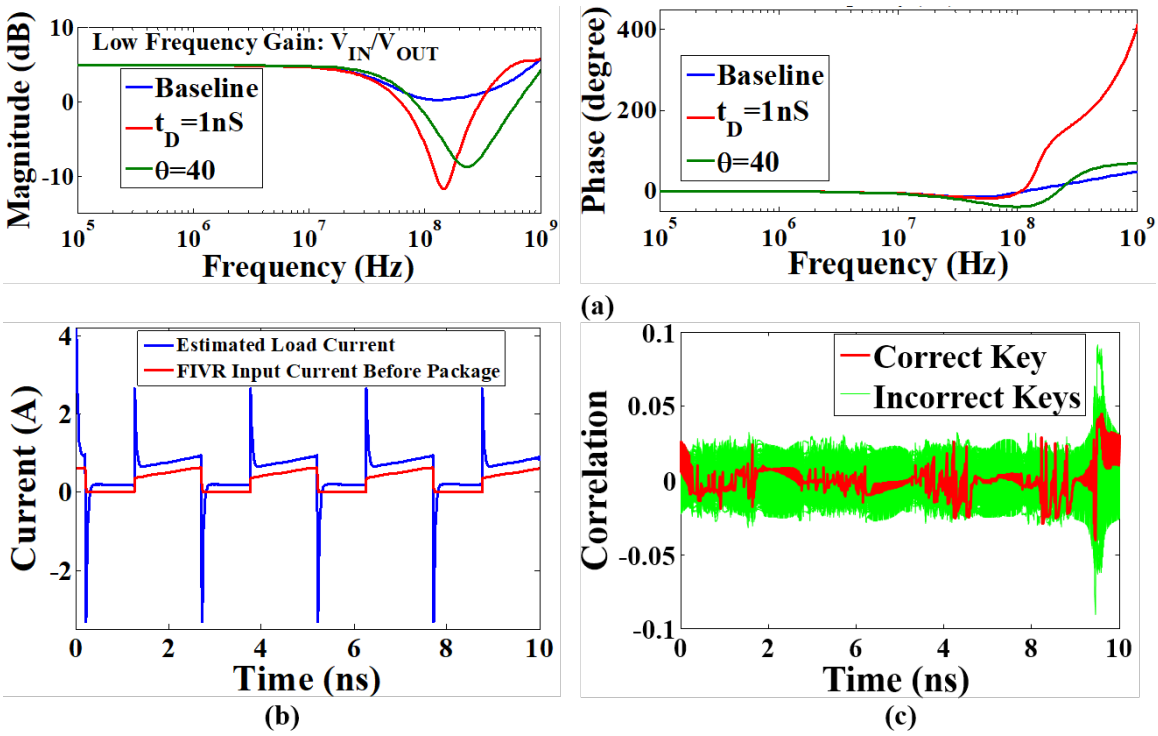

Figure 3.16: (a) Reversibility transfer function for the baseline IVR and two IVR configurations with different security aware design techniques (b) Estimated load current in time domain using RTF (c) Attack using RTF on IVR design with t_D =1ns

To generate the estimated load current, the RTF can be used as a linear system with the measured IVR input current as input to the system. However, for nonzero controller delay, Eqn. 3.12 has more zeros than poles, causing a linear simulation to fail. Algorithm 1 to estimate the load current signature from the IVR input current signature is shown below.

Results

The output of RTF in time domain, corresponding to a sample IVR input current is shown in Fig. 3.16b. The switching frequency component is not removed as the small signal derivation of RTF does not account for F_{SW}.

Similar trends as the time and frequency domain CPA are observed in an attack using

Algorithm 1 Estimation of IVR load current signature from IVR input current signature

Input:

IVR Input Signature: $[\mathbf{M}]_{\mathbf{1\times T}}$

Sampling Frequency of measurement: f_S

Window: T_{Start}, T_{Stop}

IVR Parameters: $L, C, R_L, R_C, R_O, G_C,, V_{IN}, V_{OUT}$

Output:

Estimated IVR Load Signature $[\mathbf{M_{EST}}]_{\mathbf{1\times T}}$

Begin
$CalculateRTF(s) from Eqn.3.12$
$M_{FFT} = FFT_N([M]_{1\times(T_{Start}:T_{Stop})})$
for $i = 0; i < N/2; i++$ **do**
    $F = i \times f_S/2$
    $RTF_{VAL}(i) = RTF(2\pi F)$
end for
$RTF_{VAL} = [RTF_{VAL}\ \overline{RTF_{VAL}[N/2-1:-1:2]}$
for $i = 0; i < N; i++$ **do**
    $M_{FFT,EST}(i) = M_{FFT}(i) \times RTF_{VAL}(i)$
end for
$M_{EST} = IFFT(M_{FFT,EST}) \times (T_{Stop} - T_{Start})$
return $\mathbf{M_{EST}}$
End

IVR threat model. For all the designs which did not show any positive CPA at the input current, no positive CPA was observed in the estimated load current as well, using the adversary model (Fig 3.16c).

3.8 Summary

The transformations through an inductive IVR significantly reduce the correlation between the load current signatures and the input current signatures. The correlation values can be improved through post-processing techniques like envelope or duty cycle measurements. Performing a power attack, however suggests that a reduced value of correlation does not always translate to improvement in PSCA resistance as a successful CPA was observed at the input current signatures of an illustrative IVR design. Several IVR parameters are identified which modulates the PSCA resistance at IVR input. Alternative attack modalities like frequency domain CPA or inverse transformation on the IVR input current signature

do not alter the improvement in PSCA resistance. All these results suggest that IVRs can be exploited for improvement in PSCA resistance of encryption engines [87]. The next chapters focus on the circuit details of a test-chip which would be used to characterize the improvement in PSCA resistance.

CHAPTER 4

ALL-DIGITAL INDUCTIVE IVR ARCHITECTURE

Exploiting inductive IVRs for PSCA protection requires integration of the IVR in the same process node as the digital circuits. Due to the usage of low passives, IVRs potentially can achieve a higher bandwidth, provided that the IVR controller is not limiting the bandwidth [88, 41, 1, 54, 52, 53, 42]. At advanced process nodes which are optimized for digital operations, designing high bandwidth analog PWM controller is challenging. Digital PWM control for IVRs on the other hand facilitates on-chip integration with digital cores as the entire controller uses only digital logic. Digital controllers can also exploit an advanced process node by clocking the compensator at a higher operating frequency (F_{SAMP}) to achieve a higher bandwidth [55, 50, 51]. However, the switching loss limits the maximum switching frequency (F_{SW}) and the achievable loop unity gain bandwidth (UGF) for a single phase IVR. Krishnamurthy et. al. in [50] has shown that bandwidth of a single phase IVR can be increased by using phase shifted clock, but requires a fast analog-to-digital converter (ADC) with conversion time much lower than the sampling clock period. An alternative approach to enhance bandwidth for a given switching frequency is multi-sampling, which is widely used for low-frequency ($\sim$1MHz) IVRs with off-chip passives [89, 90]. However, multi-sampling for a high frequency ($\geq$100MHz) inductive IVR imposes strict timing constraints on the digital compensator. Therefore, enabling multi-sampling in high-frequency IVRs is an important problem to address.

The integrated inductor technologies like magnetic interposer [59], magnetic thin films [60], on-chip spiral inductors [58, 51] can have higher variation than discrete (packaged) inductors. The variations in inductance and capacitance degrade the steady state power quality and responses to transient events like a load step or a power-state change [40]. The challenge is exacerbated in IVRs where the switching frequency is limited by the power

efficiency, as the filter poles ($\sim$10 to 30 MHz) can lie close to UGF making loop characteristics more sensitive to variation in the passives [55, 50]. Auto-tuning of the control loop is used in low-frequency ($\sim$1MHz) off-chip VRs to tolerate variations [91, 92]. However, the prior approaches use complex algorithms to characterize and tune frequency response of VRs which require significant hardware resources and are inefficient for realization in high frequency ($\geq$100MHz) IVRs. Hence, there is a need for auto-tuning algorithms that can be easily integrated with digitally controlled high-frequency IVRs to tolerate variations. A digital controller architecture can reduce the effect of variability on the controller, improving the overall robustness.

In this chapter, an all-digital architecture of fully integrated IVR is presented which can be easily integrated with a digital system containing an encryption engine. The all-digital controller with the on-chip auto-tuning engine is fabricated in 130nm CMOS and measurement results are presented.

4.1 Proposed Architecture

An IVR architecture is proposed with the following attributes as shown in Fig. 4.1.

- A reduced precision of coefficients is introduced to allow the compensator to use multi-sampling, without any timing failure, to improve bandwidth.
- A fast and compact (low area) auto-tuning architecture is presented to enhance tolerance to parametric variations in the filter passives without complex computation.
- An all-digital discontinuous conduction mode (DCM) controller is proposed to sense a small negative inductor current and improve low-load efficiency of the IVR
- A resistive transient assist (RTA) scheme is proposed to improve the IVRs response to large load and power state transients.

An all-digital design approach is adopted to realize different blocks of the proposed architecture i.e. most of the controller can be synthesized using standard synthesis process

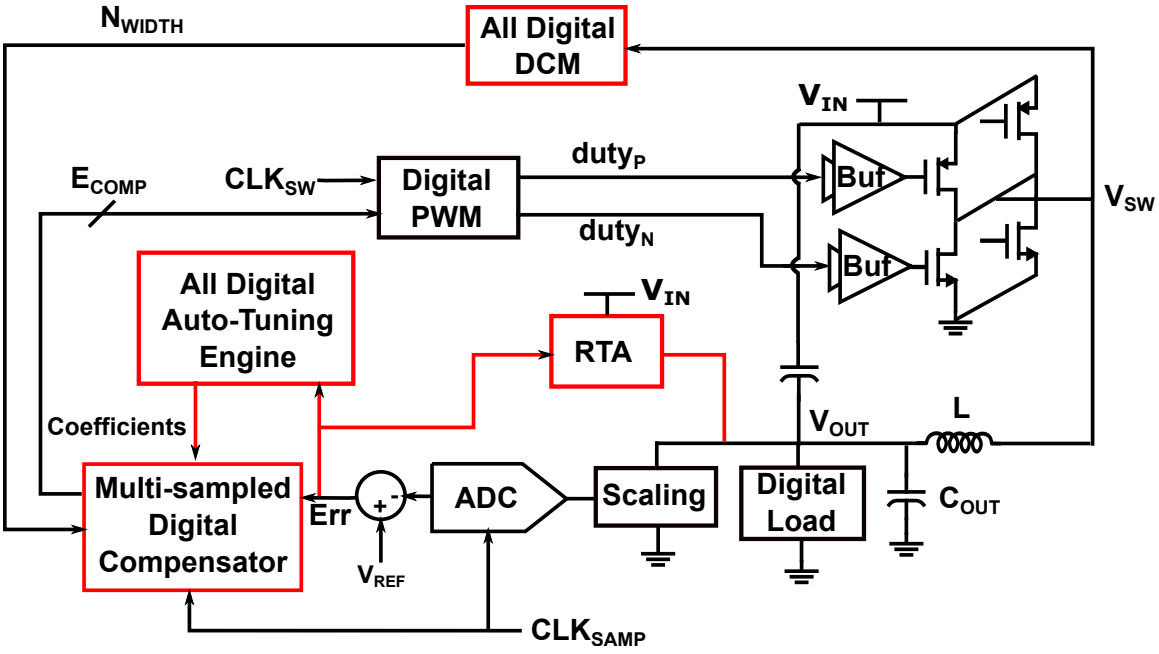

Figure 4.1: Architecture of the proposed All-digital Fully Integrated IVR Architecture

and facilitates the integration of the IVR with the digital cores (referred to as the digital load in Fig. 4.1) in advanced process nodes.

4.2 Bandwidth Improvement

A fixed-point arithmetic with computation in reduced precision is used to enable multi-sampling even at a relatively high (80 FO4 delay in 130nm CMOS) sampling frequency. Inductive IVRs use low output capacitance, which causes the capacitor ESR zero ($\frac{1}{2\pi C_{OUT} R_C}$) to reside at a higher frequency. Hence, to compensate such a power stage, a type III compensator is used as shown below:

$$G_C(z) = \frac{Comp(z)}{Err(z)} = \frac{b_0 + b_1 z^{-1} + b_2 z^{-2}}{1 - z^{-1}} \tag{4.1}$$

Given a constraint on the transient response of an IVR, the coefficients for the digital controller considering a single-cycle (F_{SW}: 125MHz F_{SAMP}: 125MHz) and a multi-cycle (F_{SW}:

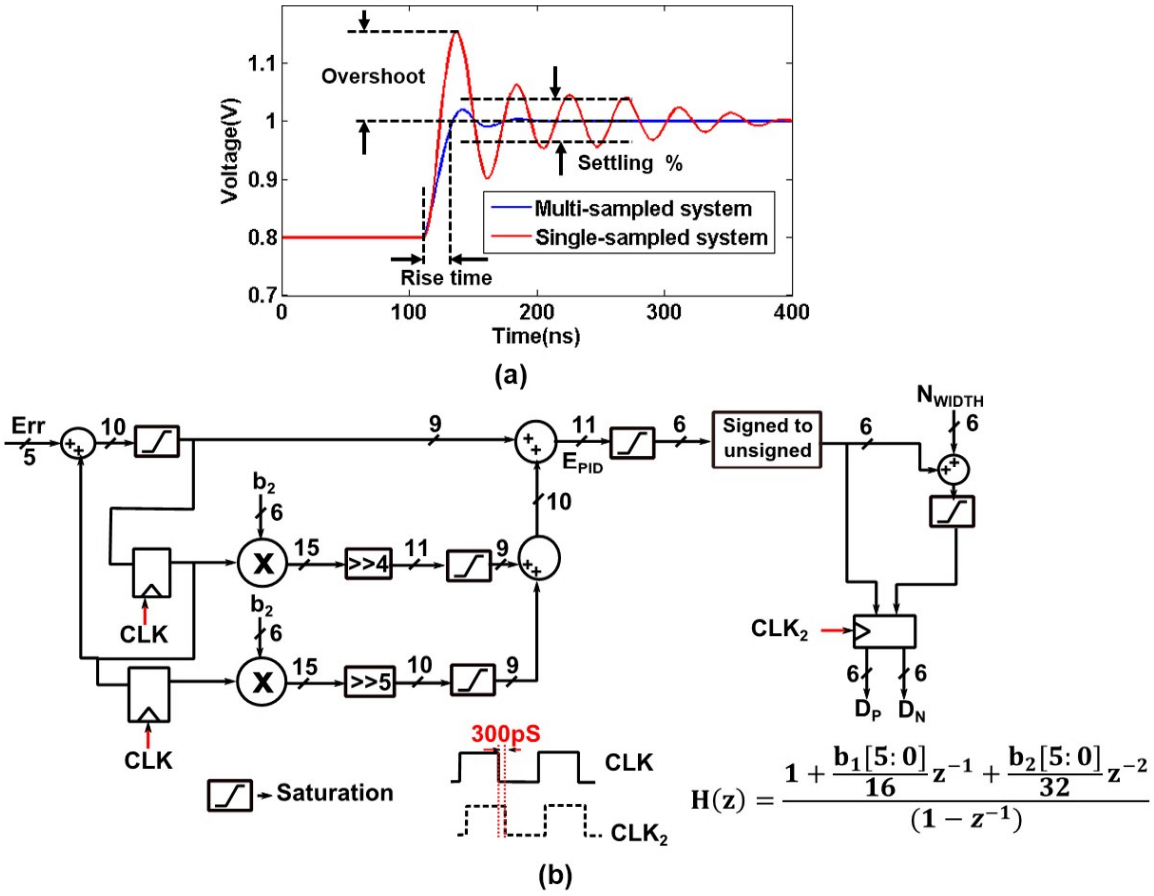

Figure 4.2: (a) Response of the single sampled and the multi sampled regulator, optimized by a Simulink based response optimization tool (b) Implementation details of the multi-sampled compensator with a 250 MHz clock

125MHz F_{SAMP}: 250MHz) operation. A multi-sampled operation with reduced-precision of the coefficients (b_0, b_1, b_2) can help the IVR to meet a tighter performance constraint indicating a higher bandwidth of the loop. First, the coefficients are optimized using a Simplex optimization algorithm. Next, the digital controller is designed using reduced-precision to meet 250MHz timing, and the quantized coefficients are used to estimate the transient performance.

The optimization process considers a 0.8V to 1V output voltage step response. The target rise time (80% change in output voltage) is 20ns, the target settling time (time re-

quired to reduce output swing below 18% of V_{DD}) is 50ns, and the target overshoot and undershoot are 5% and 10% of the output voltage, respectively. The single sampled system failed to achieve the target (best coefficients found were b_0:1.443, b_1:-0.725 and b_2:0.6503). The multi-sampled system can meet the target with a 5 bit fixed point representation and the optimized coefficient values for the multi-sampled case are b_0:1.125, b_1:-1.3750 and b_2:0.75. The multi-sampled controller with reduced bit precision shows better transient response than the single sampled controller (Fig. 4.2a). Fig. 4.2b shows the architecture of the multisampled compensator. The coefficients b_1 and b_2 are quantized as multiples of 1/16 and 1/32 (each represented using a 6 bit signed number), whereas b_0 is approximated as 1. The saturated compensated error (D_P) represents the pulse width of the PFET, whereas N_{WIDTH}, generated from the DCM engine, represents the pulse width of the NFET. A 300ps skew is used in the clock of the final stage to meet timing.

4.3 All-Digital Auto Tuning

The time domain (stable steady-state and fast transient response) behavior of an IVRs output determines a systems (digital core + IVR) performance [93]. An optimization cost, referred to as stability-figure-of-merit (SFOM) is proposed to quantify the time-domain behavior of the IVRs output. SFOM is computed by performing a set of simple arithmetic operations on the output error and the locations of the compensators poles and zeros (dictated by the compensators coefficients) are used as the tuning knobs (Fig. 4.3a). The algorithm finds the minimum SFOM over a range of coefficients applied to the system while observing the output error (digitized difference between the output and the reference). The simplicity of the resulting tuning algorithm allows a light and fast tuning engine, able to operate at F_{SW} and removes requirement for storing any error samples (Fig. 4.3b). The use of saturated adders approximates SFOM for unstable/slow responses, and computes SFOM accurately for near-optimal responses. The SFOM metric uses the following quantities: 1) absolute error (AE), calculated as the accumulation of absolute values of the error signal,

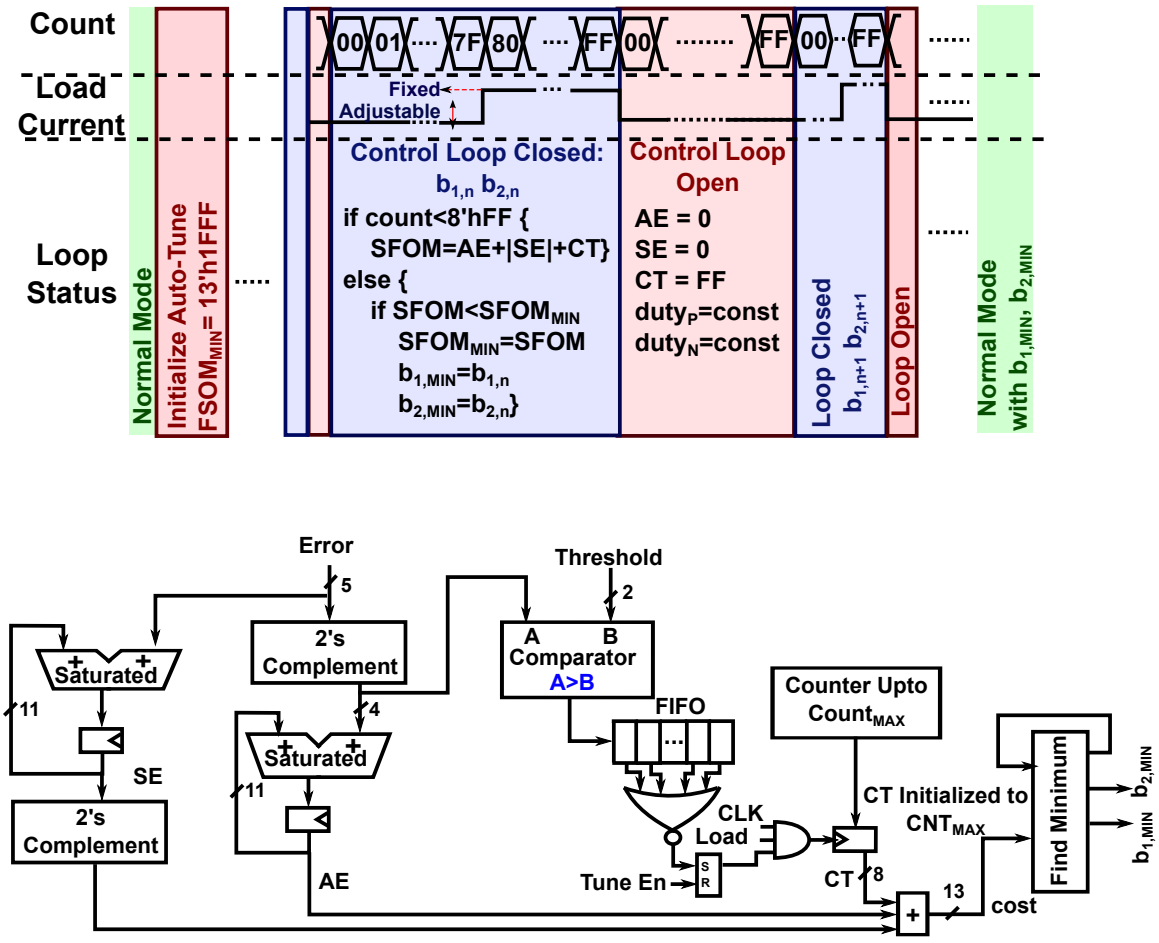

Figure 4.3: Control flow (top) and hardware implementation (bottom) of the proposed auto-tuning engine of the proposed engine

2) signed error (SE), calculated as the accumulation of signed error values, and 3) convergence time (CT). The CT quantifies the recovery time of the output from a droop caused by a load step. The CT calculation starts when a load transient is induced at the midpoint of the evaluation phase. The recovery is defined when the output is observed to remain within a user provided threshold (CT_{TH}) for ten (10) consecutive cycles. Fig. 4.4 shows the output response of a baseline IVR for three different coefficients applied, the corresponding digitized error and the different components of the SFOM. The AE helps to reject responses that are unstable for a steady load current. For the given examples, the AE is significantly

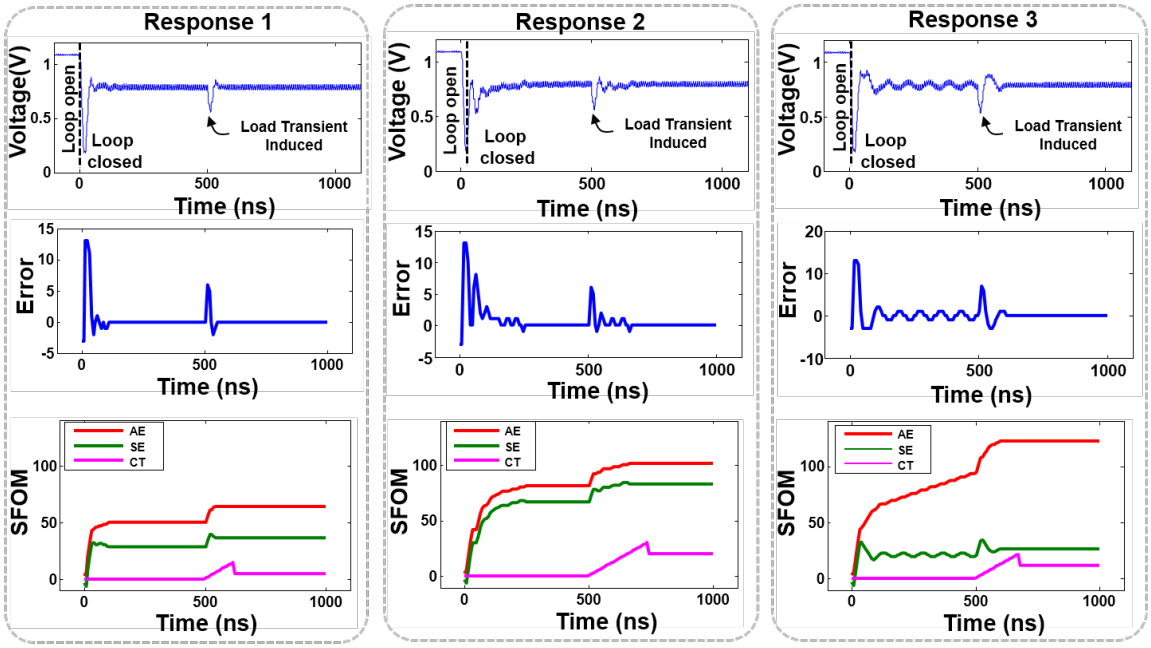

Figure 4.4: Behavior of the individual components of SFOM for different response types

higher for response 3 than response 1 and 2. The SE helps to reject responses that show damped oscillations while recovering from a transient. If the output oscillation does not dampen due to either a low phase margin (ϕ_M) or a steady state limit cycle oscillations (LCO) or complete instability, the SE remains low as +ve and ve error cancel each other. For the given example SE is higher for response 2 than response 1 and response 3. The CT selects responses with the shortest recovery time which, for the given example, is response 1. For the example response set, the tuning engine will select response 1. The SFOM metric for each coefficients, selected from a set of coefficients, is evaluated for a fixed number of sampling clocks; followed by opening the feedback loop, and driving by a fixed duty cycle to ensure the same initial condition for the next coefficients. The steady state responses are observed using two DC loads. A synthetic on-chip load generator is used to generate a fast transition between the two DC loads. The transition from open loop to closed loop is used to emulate the reference transition.

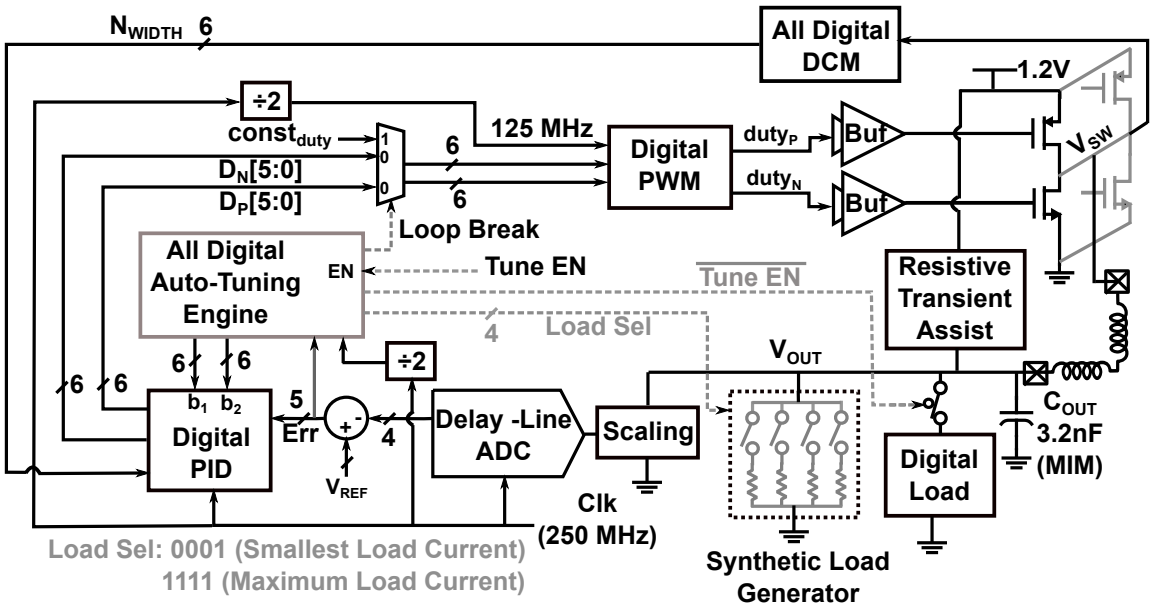

Figure 4.5: Detailed system architecture of the 130nm integrated voltage regulator

4.4 System Implementation

The detailed architecture of the proposed IVR is shown in Fig. 4.5. Package bondwires are used as the power-stage inductor and an on-chip MIM capacitance as the output filter. Based on the package datasheet, the total bondwire inductance is estimated to be 11.6nH. A delay-line based ADC is used for digitizing the output. The digital compensator, the auto-tuning engine and a serial interface for programming are generated with digital synthesis tools. The compensator output is fed to a delay locked loop (DLL) based DPWM engine. The regulator can operate in an open-loop condition where the DPWM is driven by a fixed input word, generating gate signals with a constant duty cycle. An all-digital DCM engine and an RTA circuit are added to the IVR. A voltage-controlled-oscillator (VCO) generates the multisampling clock that is distributed to the ADC and the controller. The DPWM clock (F_{SW}) is derived from the compensator clock (F_{SAMP}) to ensure that the duty cycle commands from the controller (D_N and D_P) change synchronously with F_{SW}.

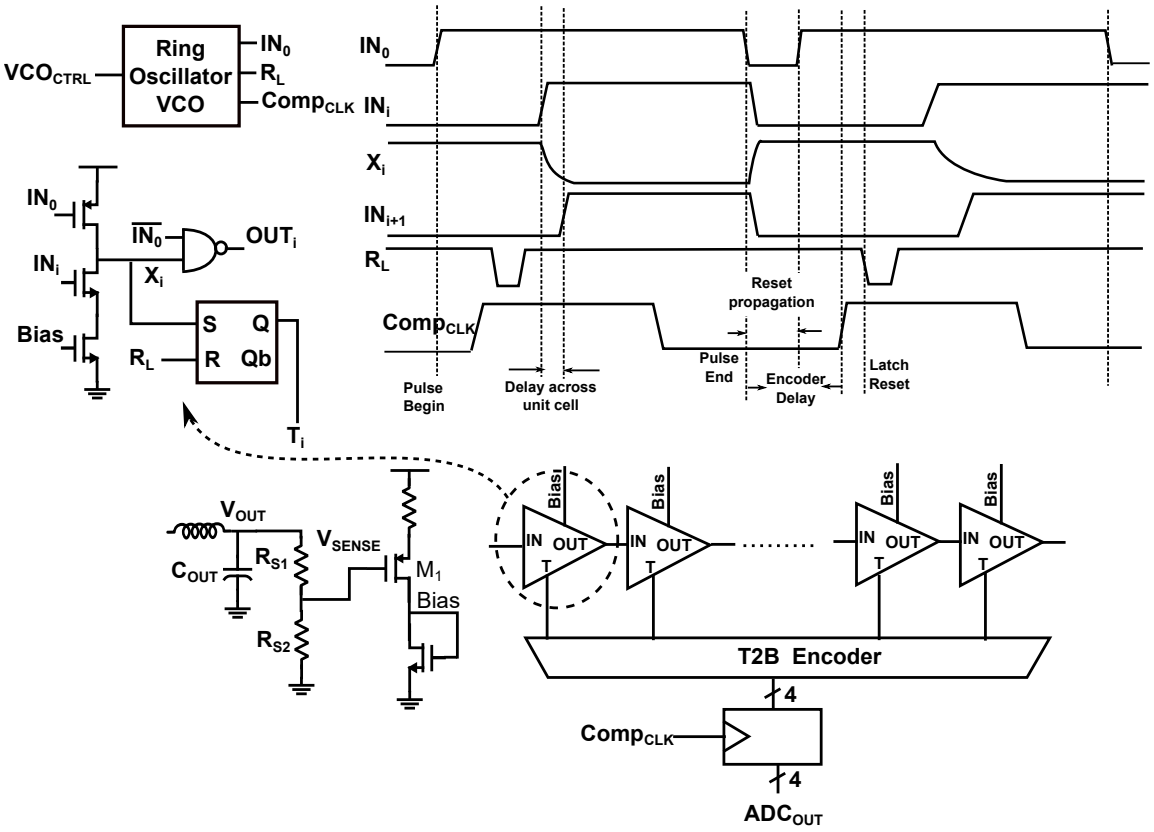

Figure 4.6: Architecture and corresponding elements of the implemented delay-line based ADC

4.4.1 Delay-line based ADC

The small-signal gain through an ADC in a digital controller can be expressed as

$$G_{ADC}(s) = \frac{1 - e^{-sT_s}}{sT_S} \times \frac{1}{v_{LSB}} \times e^{-st_{D,ADC}} \tag{4.2}$$

where T_S is the ADC sampling clock, v_{LSB} is the voltage change corresponding to 1 LSB change in the ADC output and $t_{D,ADC}$ is the ADC conversion delay. The ADC requires a high sampling speed to reduce the feedback delay ($t_{D,ADC}$) and a higher resolution for more accurate binning of the output voltage. Multi-sampling imposes more stringent constraint on the sampling speed, which can conflict with the resolution. Fig. 4.6 shows the delay-

line based ADC architecture [94] used in the proposed IVR. The entire design, except for the sense branch, is synthesizable. The current mirrored from the sense branch, consisting of a source degenerated PMOS (M_1), controls the delay of the current starved inverter in each stage. A conversion cycle begins by initiating a pulse with high duty cycle (IN_0) at the input of the chain and ends when IN_0 goes to logic zero. During the conversion time, depending on the delay of the cells, the input pulse crosses a partial number of delay cells, before IN_0 goes low. Each delay cell also contains a RS latch that samples and stores the intermediate node (X) once it goes low. The latches are reset using the signal RL in the middle of the conversion cycle. The latch outputs are fed to a thermometer to binary encoder to obtain a binary format output. Having the intermediate latches ensure that the computation delay through the T2B encoder does not affect the operation of the main delay chain. The T2B output is sensed by the compensator clock ($COMP_{CLK}$) right before RL goes low. Moreover, the delay between the positive edges of IN_0 and $COMP_{CLK}$ is less than the delay through the T2B encoder, ensuring no hold violations.

4.4.2 Limit Cycle Oscillation

A limit cycle oscillation (LCO) is a well-known problem in digitally controlled buck regulators and is caused by the finite granularity of the DPWM engine. A LCO is traditionally avoided by satisfying three conditions [95]:

1. A lower voltage resolution of the ADC than that of the DPWM engine
2. Setting the integral gain of the compensator less than unity
3. ensuring loop stability with the highest small signal gain across the ADC

In a single-sampled system, the ADC sampling clock always samples the output ripple at the same location and therefore the ripple magnitude doesn't play any role in inducing a LCO. In a multi-sampled controller, the output voltage is sampled, typically using a sample-and-hold circuit (S&H), multiple times in one switching cycle. If the peak and trough of

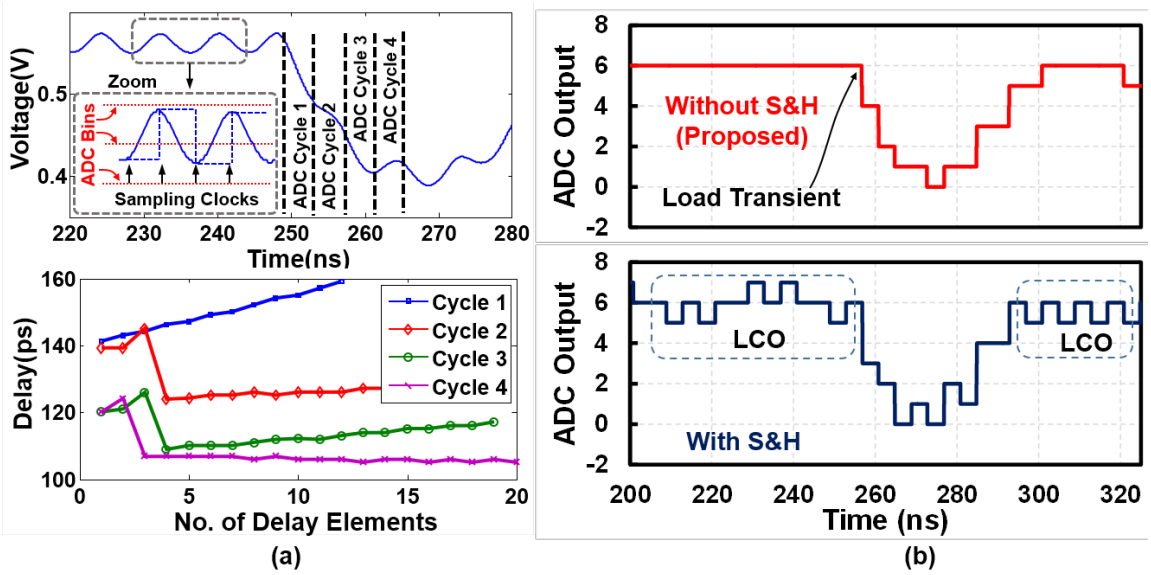

Figure 4.7: (a) Delay variation in the unit cells for changing output (droop during a load transient) for four consecutive conversion cycles for the proposed design (no S&H before ADC) with a scaling factor of 1 (b) Comparison of steady state response of the output for the proposed design (no S&H before ADC) against a traditional design (S&H before ADC)

the output ripple is sampled and peak-to-peak ripple magnitude maps to different ADC bins (Fig. 4.7a inset), a LCO can occur, even if the other conditions are satisfied. This adds a fourth criteria of avoiding LCO for multi-sampled controllers.

The proposed ADC design does not use a dedicated S&H circuit, instead uses latches within the delay cells working as an intermediate storage element (Fig. 4.6) and addresses the fourth criteria of avoiding a LCO. Consider that the IVRs output voltage (i.e. ADC input) changes at the middle of a conversion cycle. Consequently, the delay of each of the delay elements will change (Fig. 4.7a), but the states of the delay elements that have already flipped are stored in the corresponding latches. This effect causes the effective sampling frequency of the output to be 1/delay of the unit cells (i.e. higher effective bandwidth of the ADC gain). The total number of delay cells that changed its states i.e. the ADC output depends on the average value of the sensed voltage during the ADC conversion cycle

instead of the sampled value of the sensed voltage at the beginning of the ADC conversion cycle, if a dedicated S&H was used. This achieves the same effect as an antialiasing low-pass filter or a Repetitive Ripple Estimation [90] without increasing feedback loop delay. Fig. 4.7a also shows the delay of the consecutive cells during a voltage droop at the IVR output for the proposed ADC design for four consecutive ADC conversion cycles. As the output droops during cycle 1, 2 and 3, the delay between consecutive cells increases during the conversion cycle. For cycle 4, the sensed voltage stays relatively constant, and therefore the delay does not change significantly between consecutive delay cells. The simulations also show that introducing a S&H at the input can causes limit cycle oscillation (LCO) at the output, but the proposed design (no S&H) does not show any LCO (Fig. 4.7b). The first and the third criteria for avoiding a LCO are satisfied during the design phase. LCO can still occur from the selection of the compensator coefficients or due to passive variations which increases the peak-to-peak output ripple and the sampled outputs in one switching period map to different ADC bins. The proposed auto-tuning engine can correct for the second criteria, however avoiding LCO under increased ripple requires adjusting the scaling factor before the ADC.

4.4.3 All-Digital DCM

An all-digital DCM engine is used to improve the light-load power efficiency of the IVR. The existing digital DCM controllers for high frequency IVRs sense the V_{SW} node after the NFET turns off and reduce the width of the NFET pulse till the sensed value becomes logic 0 [96]. However, smaller negative I_L results in a long rise time of the V_{SW} node and may not be detected by digital sensing (Fig. 4.8a). To address this challenge, the falling edge of the NFET is used to create multiple (delayed) sampling clocks which are combined using an OR gate (Fig. 4.8b). Multiple sampling of the V_{SW} node facilitates detection under parametric variation even at small negative I_L. Another layer of flip-flops, clocked by the inverted PFET gate signal, samples the outputs of the first layer of flip-flops clocked by the

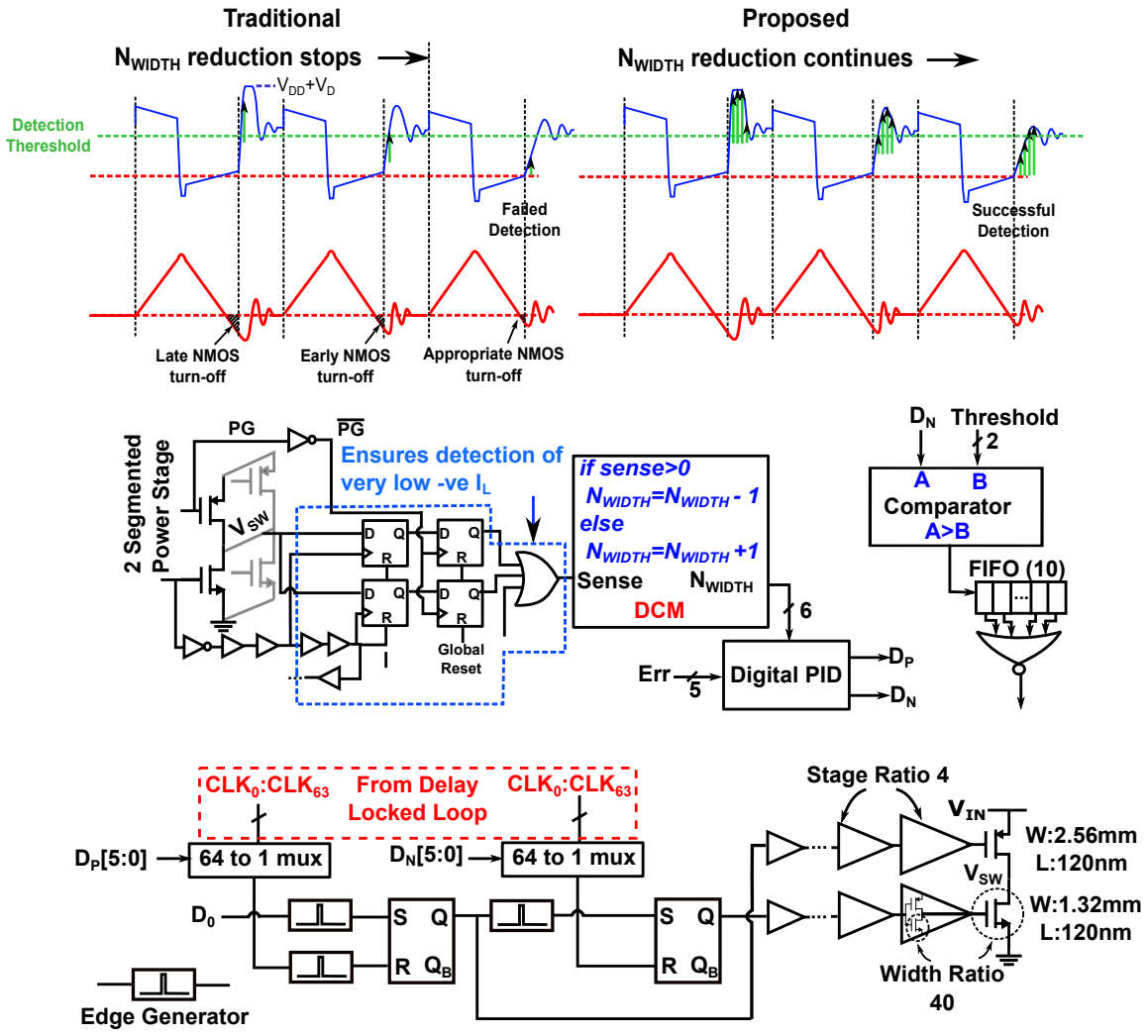

Figure 4.8: (a) The effect of multiple sampling of the V_{SW} node after the NFET turns off. (b) Proposed all-digital DCM controller and (c) DPWM architecture and power stage

sampling clocks. This is necessary to prevent a false detection of the V_{SW} node after the PFET has turned on for the next cycle. Sensing using only the last sample might not be accurate if the time interval when both the FETs are turned off is not enough to complete all 4 samplings. The DCM engine senses the ORed result and outputs a digital word (N_{WIDTH}), which keeps on decreasing till the sensed value is logic 0. Fig. 4.8c shows the gate signal generation from the DPWM and implementation of the power stage and the drivers. A 64-

stage delay locked loop (resolution of 125ps) with two 64-to-1 mux are used to generate the driving signals for the power FETs from the words D_P and D_N. The widths of the power FETs and the drivers (details in Fig. 4.8c) have been optimized to maximize power efficiency at 70mA load current as well as the ability to pass a thin pulse ($\leq$ 1ns) for skewed duty cycles. To improve the light-load efficiency, the power stage is split into two segments. In DCM mode, if D_N falls below a threshold value (A_{WIDTH}) for 10 consecutive cycles, one of the power FET segments turns off, and reduces the driving loss (Fig. 4.8b). Fig. 4.9a shows the inductor current and the delayed samples of the V_{SW} node for CCM to DCM transition through simulation. As the NFET pulse width reduces, the latter samples can detect negative I_L (although the initial samples fail) and help reduce N_{WIDTH} until detection fails for all samples. Fig. 4.9b shows that N_{WIDTH} values for different sampling options continuously oscillate. When the sensing logic detects a logic 0, N_{WIDTH} starts increasing till a logic 1 is detected again. This causes the N_{WIDTH} to continuously toggle within a set of values. As more samples are used in the sensing process, the average N_{WIDTH} value reduces and eventually saturates to a minimum value improving power efficiency (Fig. 4.9c)

4.4.4 Resistive Transient Assist

A transient assist scheme, referred to as Resistive Transient Assist circuit (RTA) is introduced to reduce response time of load or reference transients (Fig. 4.10a). The proposed scheme uses transistors M_{T1} and M_{T2} to assist the output directly from the input voltage, bypassing the inductor and the control loop. The transistors are driven by digital comparators that compare the digitized error, already available from the compensator block, with two threshold values. If the errors are positive i.e. the output is less than the reference, and more than the threshold value of the corresponding comparator, the switch turns on and assists the output by supplying current directly from the input. The current assist from the input to the output scales with the droop magnitude. This is achieved by keeping multiple (two) assist devices (equal width) where both the devices turn on only when the droop exceeds

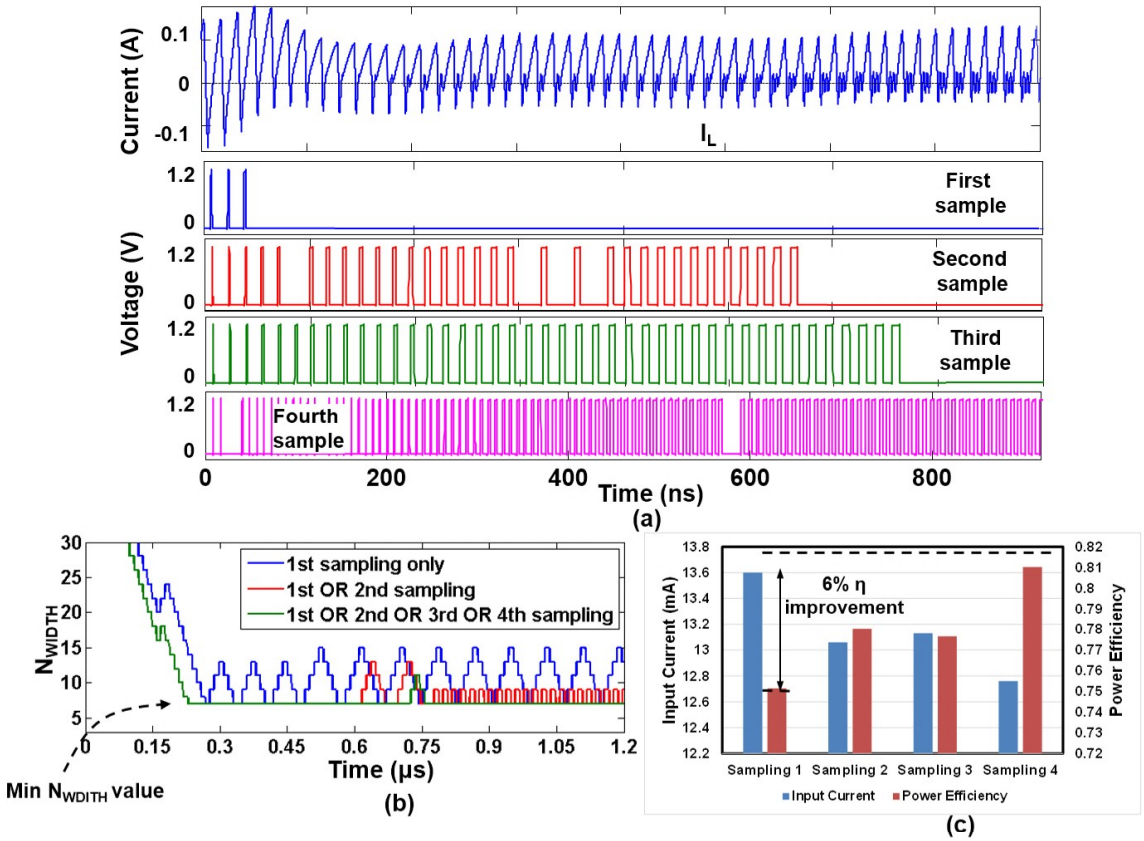

Figure 4.9: (a) Simulated waveforms of the inductor current and the V_{SW} sense outputs while transitioning from CCM to DCM (b) N_{WIDTH} against time for different sampling methods for CCM to DCM transition and (c) corresponding improvement in power efficiency (conduction loss only)

the larger threshold. No hysteresis was added to the comparator to avoid overshoot of the output voltage beyond the maximum tolerable value. The threshold values are chosen to ensure that the maximum positive error during a LCO does not trigger the RTA. Fig. 4.10b shows that enabling the RTA (WM_{T1} =WM_{T2} =100m) helps reducing voltage droop due to a load step (20mA to 100mA) by 50mV. Increasing widths of the assist devices reduces the voltage droop, but the settling time increases. A stronger assist reduces the digitized error at the output (compared to no RTA), which reduces the control effort of the compensator

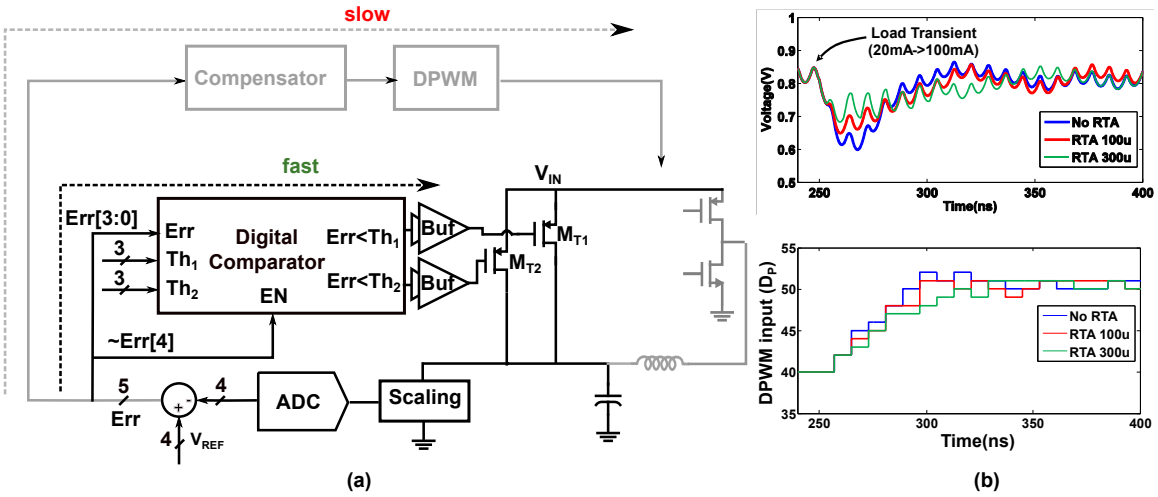

Figure 4.10: (a) Architecture of Resistive Transient Assist (b) Effect of varying width of the assist devices (M_{T1} and M_{T2}) on droop and settling time of load transient (Th1=3b010,Th2=3b011)

resulting in lower output slew when the RTA turns off.

4.5 Measurement Result

The integrated buck regulator was fabricated in 130nm process and packaged using a wire-bond Ceramic Leadless Chip Career (CLCC) (Fig. 4.11, Table I). The power stage operates at 125MHz and can convert 1.2V to 0.45V-1.05V output. The minimum output is limited by the lower range of the ADC input. Scaling factors are appropriately adjusted to ensure that the scaled outputs are within the ADC range. The output characteristics and the control loop of the IVR are characterized by operating the power stage in the open loop condition, with varying DPWM input in steps of 1 with zero load current (Fig. 4.12). The DPWM provides a linear input code (6-bit word) to output voltage profile. The average peak-to-peak ripple is measured to be 84mV. The corresponding ADC output shows three key observations. First, the ADC goes through all possible states for increasing DPWM code and multiple DPWM codes map to the same ADC bins for most of the ADC states.

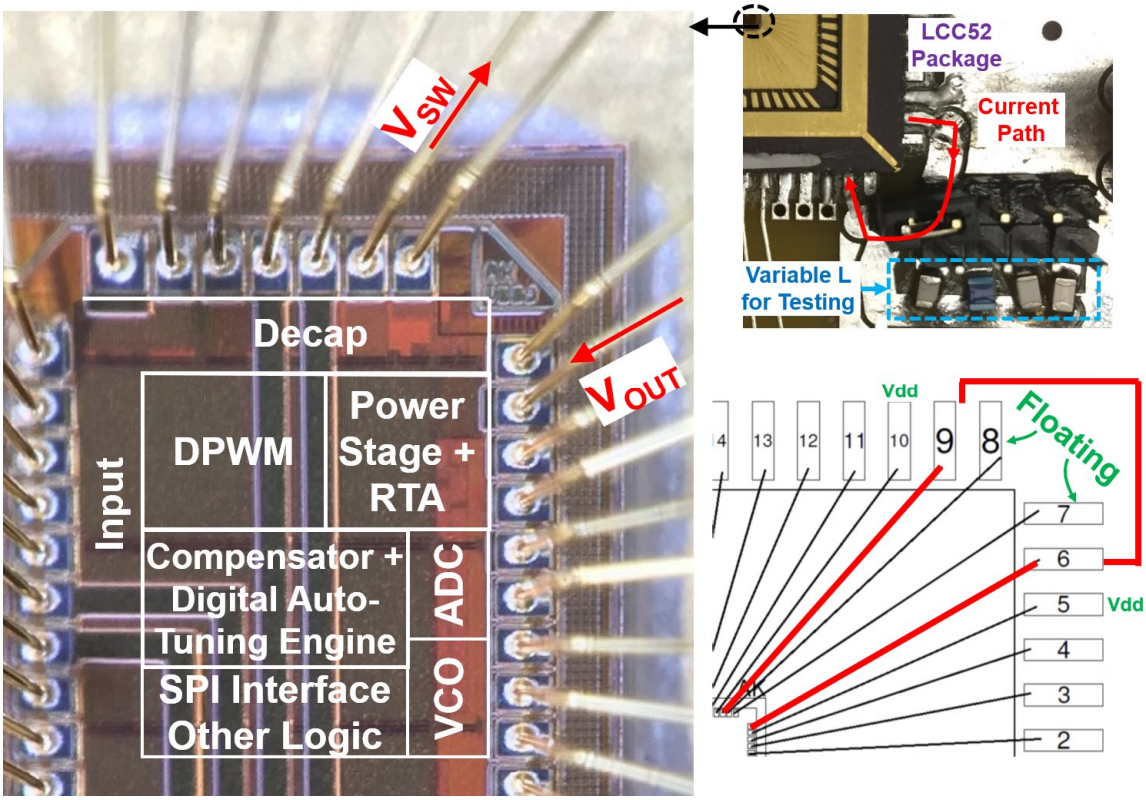

Figure 4.11: Micrograph of the chip and corresponding package and board level assembly for testing

The result indicates that the ADC resolution is less than DPWM resolution which satisfies the first criteria for reducing LCO [95]. Second, the ADC shows non-linearity near a low output voltage. This is due to the non-linearity of the delay of the ADC delay elements with respect to the control voltage. The loop stability is not affected when the ADC gain is highest (around 800mV output) which satisfies the third criteria for reducing LCO [95]. Finally, the peak-to-peak ripple for a fixed DPWM code spans across 3 different ADC bins, however the ADC output remains fixed across multiple measurements, due to use of the delay line based ADC and absence of a dedicated S&H as explained in section 4.4.1.

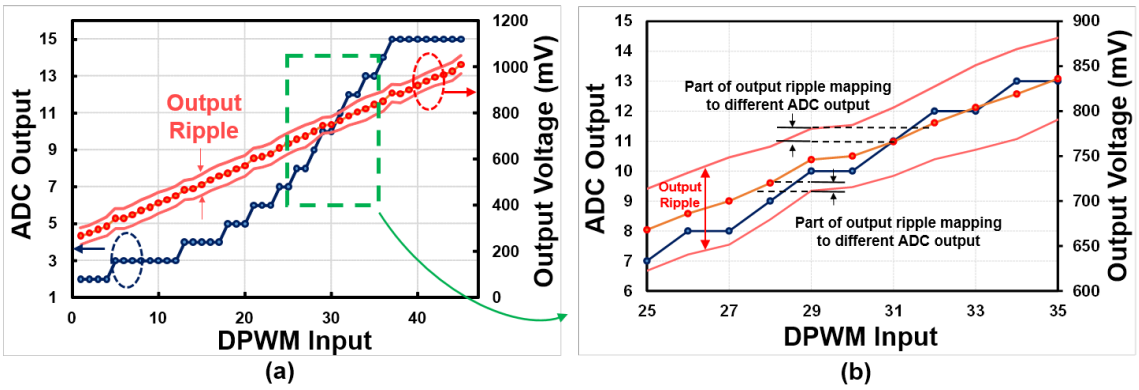

Figure 4.12: (a) Characterization (measurement) of the control loop: output voltage and ADC output for varying DPWM input in open loop condition (b) Span of peak-to-peak output ripple across different ADC LSB levels

4.5.1 Auto-Tuning of Coefficients

The power stage inductance is formed by two bondwires in the 52 pin CLCC package, shorted externally through a PCB trace. Unlike the bondwire formation in [52], the package and an external low resistance PCB connection is included in the inductance path, similar to [49]. The average bondwire length is 5.5mm, providing an average of 5.8nH per bondwire, estimated based on the package datasheet. The inductance offered by the package is expected to be minimal due to absence of leads. The bondwires near the corner of the die are chosen to extract the maximum inductance and to keep maximum distance between the inductance forming bondwires to avoid negative mutual inductance effect [49]. One of the adjacent bondwires for each inductance forming bondwires are kept floating to also reduce mutual inductance (Fig. 4.11). However, the other adjacent bondwires, which themselves are subjected to variations, play a role in mutual inductance. The length of the bondwires can also vary during the bonding process. Therefore, as identified in [52], there can be appreciable variability in the effective inductance value. The authors in [52] address the impact on variability on power efficiency, however the variability on the transient

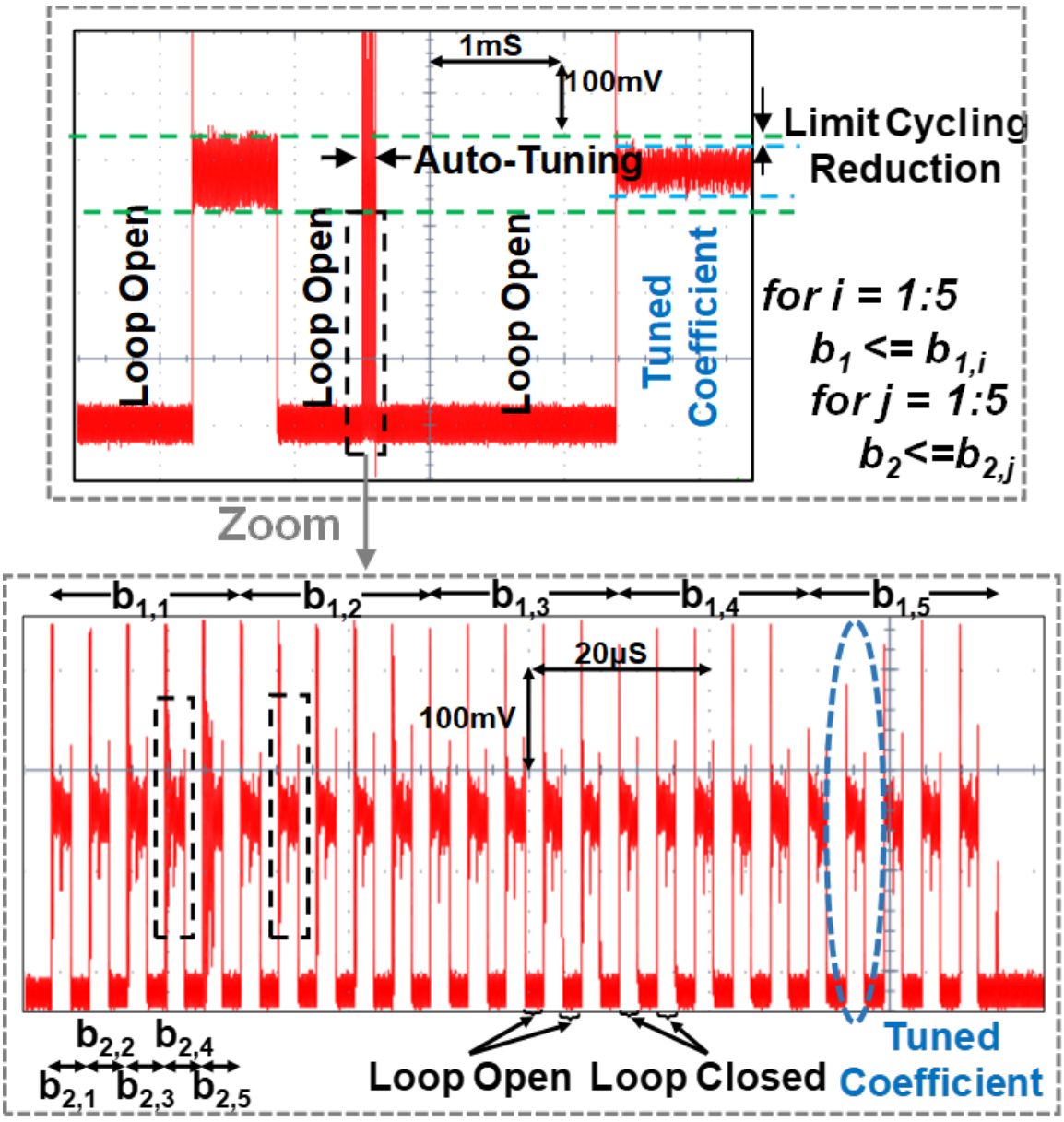

Figure 4.13: Auto-tuning operation and the corresponding waveforms

performance of the IVR is not addressed. The proposed design uses auto-tuning to address the effect of inductance variation on the transient performance.

Fig. 4.13 shows the behavior of the IVR output when the auto-tuning process is triggered using an external enable signal. The designed controller first disengages the feedback loop, followed by the tuning phase where the optimum coefficients are found and the loop

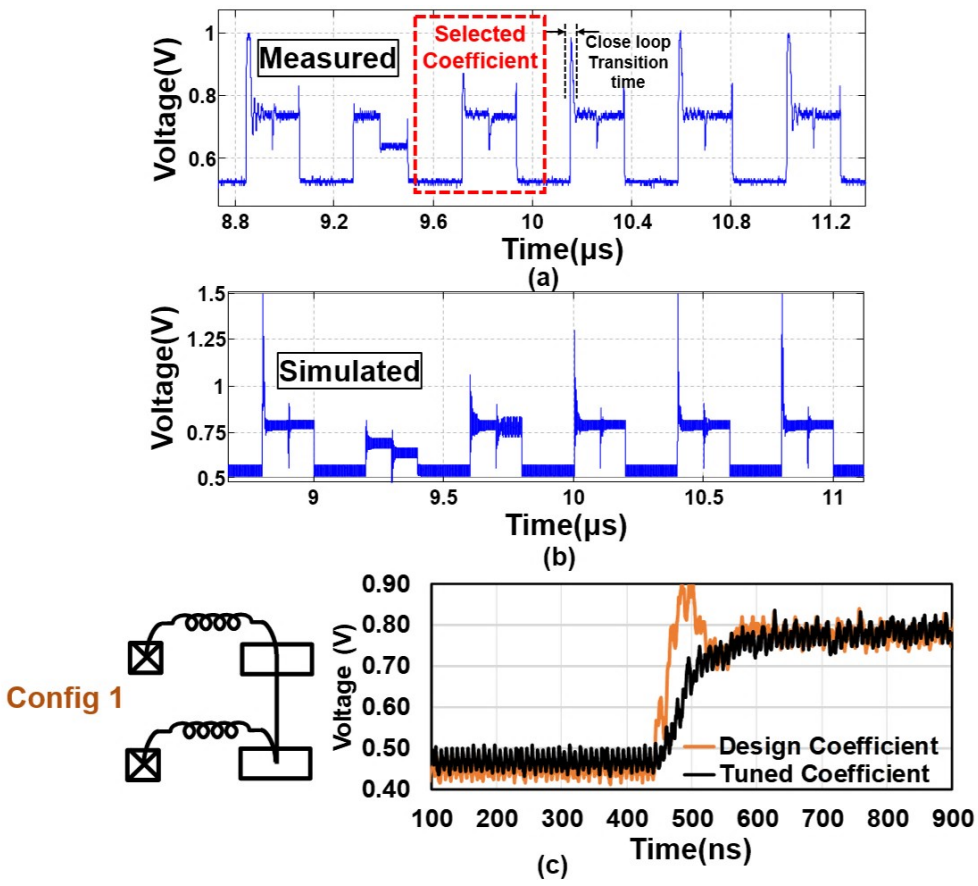

Figure 4.14: Zoomed in waveforms for a set of coefficients during an auto-tuning process from (a) measurement and (b) simulation. (c) Measured reference transient for the selected coefficients.

is subsequently closed with the new coefficients. The measured waveforms show limit cycling at the output before tuning which reduces after the coefficients are modified through the tuning process. A total of 25 different (b_1, b_2) pairs are covered during the tuning. Fig. 4.14a shows the zoomed output voltage (six coefficient pairs and responses) during the tuning. The responses measured from the test-chip are more damped than that for the modeled system in Simulink (Fig. 4.14b) due to additional resistance in the power stage. Fig. 4.14c shows the measured step response of the converter for a set of designed coefficients and the coefficients found after auto-tuning. To emulate a variation in the output inductance, an

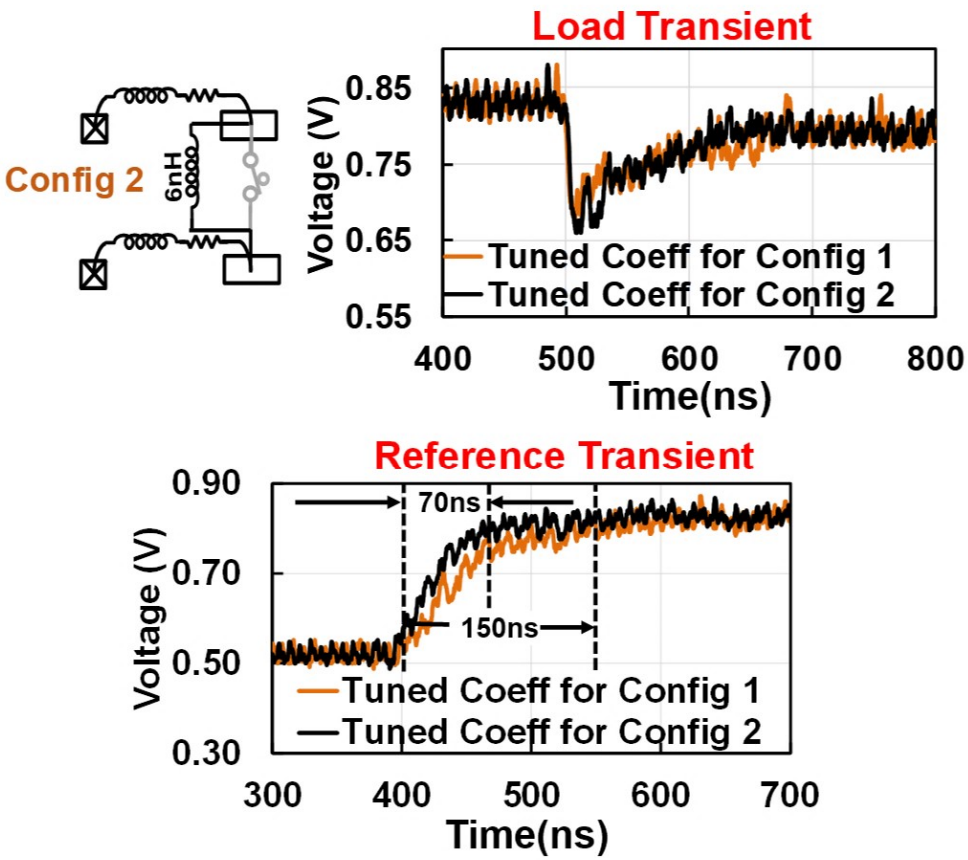

Figure 4.15: Effect of updated auto-tuning coefficients after the power stage is modified to emulate +50% variation in L.

external PCB inductance is added in series with the bondwires. An extra 6nH inductance emulates 50% variation in expected L. During the auto-tuning process, the system becomes unstable for initial few coefficient pairs, caused due to the shift of the LC poles at a lower frequency. The coefficients found for the previous configuration (Fig. 4.14c) were used to test the reference step response and load step response of the new configuration (config 2) with extra L. The updated coefficients for config 2 yields a better reference step response and a comparable load step response than the coefficients for config 1 (Fig. 4.15). This clearly shows that the tuning process needs to be performed separately for every system.

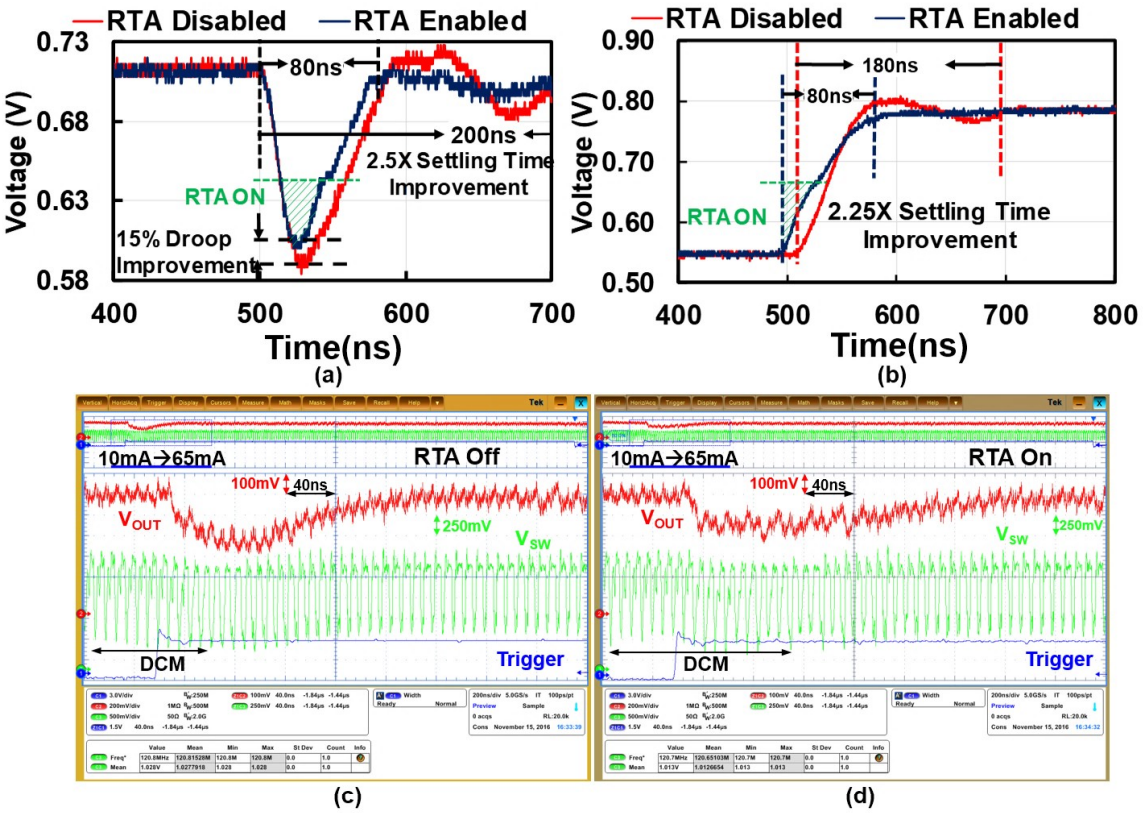

Figure 4.16: (a, b) Measured (band limited) load and reference transient in CCM mode with and without RTA active (c, d) Measured load transient from DCM to CCM, (c) without and (d) with RTA

4.5.2 Performance During Transient Events

The internal synthetic load generator is used to create fast load transients (75mA/100ps). The reference transient is generated by changing the digital reference word. The measurement results show that after enabling the RTA, the settling time for a 5mA to 65mA load transient improves by 2.5X and the voltage droop improves by 15%. Further, for a 0.55V to 0.78V reference transient, the settling time improves by 2.25X (Fig. 4.16a, b). The output slew recorded during the reference transient with the RTA on is 230mV/80ns (= 2.9V/μs).

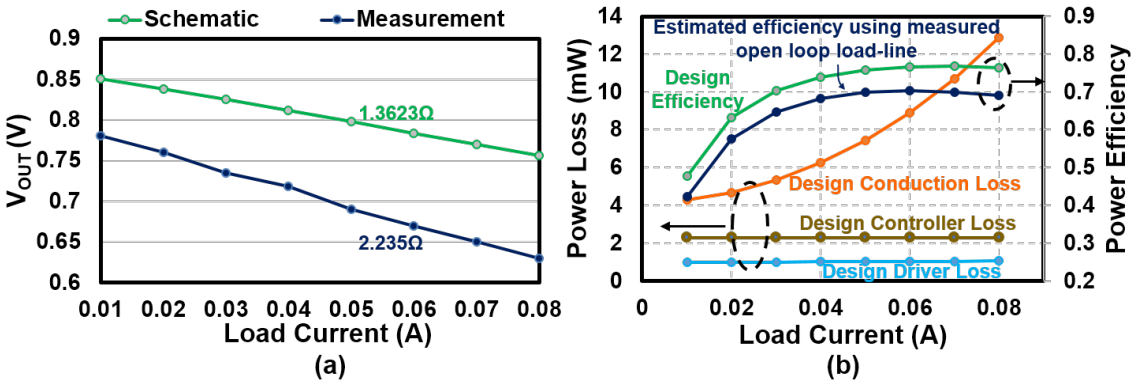

Figure 4.17: Open loop load-line for schematic and measurement (b) Simulated distribution of losses and efficiency from schematic and efficiency estimated from measured open-loop load line.

The disengaging of the RTA circuit is visible from the change in the output slew during recovery from a load transient and the initial phase of a reference step. The effect of RTA is also studied considering the IVR is initially in the DCM mode (Fig. 4.16c, d). The waveforms of the V_{SW} node, without the RTA on, show that the regulator quickly comes out of the DCM mode as E_{PID} goes high and saturates D_N (Fig. 4.2b). When RTA is enabled (Fig. 4.16d), the droop reduces, however the settling time increases. This is caused by a slower increase of D_P and N_{WIDTH}, as assist current is directly added at the V_{OUT} node, reducing the control effort. This causes the regulator to take 7-8 cycles to come out of the DCM mode.

4.5.3 Power Efficiency

Fig. 4.17a shows that the open-loop load-line resistance increases from a simulated value of 1.3623ω to a measured value of 2.235ω. The change can be attributed to the resistance of the power distribution network, shifts in the bondwire resistances, and the resistances of the package leads and the PCB connection. Fig 4.17b shows the division of conduction

Table 4.1: Performance Comparison with Previous Work

	[53] (2013)	**[50] (2014)**	**[58] (2011)**	**[51] (2016)**	**[97] (2012)**	**[61] (2017)**
Technology	130nm	22nm-Trigate	130nm	65nm	45nm	130nm
L (nH)	3-7(Bondwire)	1.5 (On-die)	2 (On-die)	1.54x2 (On-die)	26x4 (SMT)	5.6x2 (Bondwires)
C (nF)	9.8 (On-die)	10 (On-die)	5 (On-die)	1.83 (On-die)	23(Ext.)	3.2 (On-die)
$^{\$}F_{SW}$ (MHz)	100	500/500	300	500/500	80	125/250
Controller	Analog PWM	Digital PWM	Analog PWM	Digital PWM	Digital PWM	Digital PWM
Vin (V)	1.2	1.5	1.2	2.0-2.2	1.5	1.2
Vout (V)	0.9	1	0.86	1.2	0.6-1.3	0.45-1.05
Peak Eff (%)	82 (300mA,0.9V)	68 (90mA,1V)	74.4 (125mA, 0.86V)	76 (400mA,1.2V)	83 (750mA,1V)	71 (50mA,0.8V)
Improvement Over LDO (%)	5	2	3	16	17	5@0.8V Vout 10@0.6V Vout
Area (mm^2)	2.25	1.5	0.56	1.13 (1.59 including decap)	0.75	0.5 (1.19 including MIM-cap + decap)
Voltage Ramp	-	150mV/100ns	250mv/1.4s	200mV/8.3s	100mV/70ns	230mV/80ns

$:Switching frequency/Sampling frequency (for digital control)

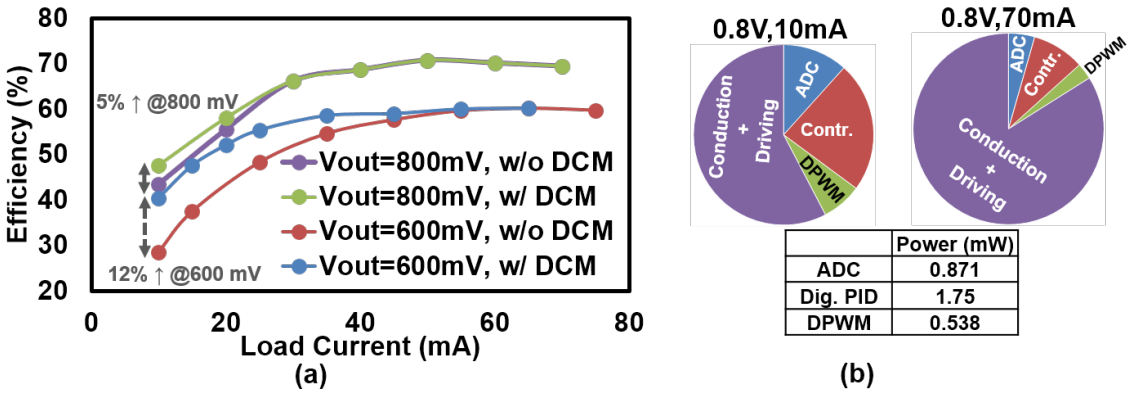

Figure 4.18: . (a) Measured power efficiency of the regulator across different load current (d) power loss breakdown at high and low load condition

loss, driving loss and controller loss and corresponding design efficiency for 0.8V output across different load currents. The difference in load-line resistances, between design and measurement is used to estimate the excess conduction loss and predict the efficiency (Fig. 4.17b) as used in [97]. The measured efficiency (Fig. 4.18a) matches closely with the estimated value (Fig. 4.17b) and shows a peak of 71% at 0.8V output @50mA. The DCM mode with adaptive power FET improves light load efficiency by up to 12% (600mV V_{OUT} at 10mA). Adaptive driver width does not kick in for 0.8V output as the threshold for driver width (AWTH) is set as 32 ($6b_100000$). For 0.6V output, adaptive driver width kicks in and increases the improvement in light load efficiency. Table 4.1 shows the comparison with prior works on high frequency inductive IVRs. The proposed design shows improved voltage ramp rate (reference transient response) compared to the previous works. Moreover, the proposed design supports auto-tuning at high operating frequency, which has not been reported in the prior works. The measured efficiency of the proposed design is lower than the previous works. The model-to-hardware correlation analysis presented in Fig. 4.17 shows that the additional resistance in the power stage is the key reason for the efficiency change from simulation to measurement.

4.6 Summary

This chapter presents an all-digital architecture of a fully integrated inductive IVR. The proposed architecture facilitates seamless integration of the IVR into a digital process node. Use of a reduced precision multi-sampled digital PID compensator turns the disadvantage of high bandwidth analog controller design into an advantage of exploiting the fast digital process to improve loop bandwidth. The all-digital DCM engine improves the light load power efficiency by precise control of NMOS pulse width. Use of a delay-line ADC allows to avoid LCO and improves the supply quality to the digital logic. The transient assist circuit improves output response to deep load transient as well as power-state transients. The proposed auto-tuning engine tunes the controller coefficients with respect to a cost function which ensures steady load stability as well as improved transient performance against variation in filter passives. This feature is also critical for the security of the entire system as an adversary might attempt to change the passives to nullify the improvement in PSCA resistance at the IVR input. In the next chapter, the PSCA resistance at the input of the proposed IVR, driving a 128-bit AES engine, will be characterized using measured data from the test-chip.

CHAPTER 5
SIDE-CHANNEL CHARACTERIZATION

The analysis presented in Chapter 3 shows that an inductive IVR can improve the PSCA resistance of a 128-bit AES engine and the improvement is dependent on the parameters of the IVR. However a simulation based analysis can either underestimate or overestimate the improvement in PSCA resistance. For example, when the PMOS of IVR's power stage is off, the load current is circulated through the NMOS internally and the simulation does not capture any leakage through the body diode of the PMOS. Similarly, as it will be shown in this chapter, another important transformation through the IVR, a misalignment caused due to the asynchronous relation between the IVR clock and the AES clock is not accounted in the simulation framework and this transformation hinders the signal alignment process, therefore the actual improvement in PSCA resistance due to an IVR might be higher. In this chapter, the improvement in PSCA resistance at the input of the illustrative IVR design, described in Chapter 4 will be characterized.

5.1 Prototype Design of an Inductive IVR and AES-128

A 128-bit AES engine is chosen as the targeted encryption engine to understand the improvement in PSCA resistance through the implemented inductive IVR in the 130nm CMOS prototype. The IVR architecture and measurement results are described in Chapter 4. The blocks of the IVR which play an important role in improving PSCA resistance are marked in red and shown in Fig. 5.1. The IVR output drives the AES engine which also has a provision to be driven by an external voltage. The switch S_1 is connected or disconnected accordingly.

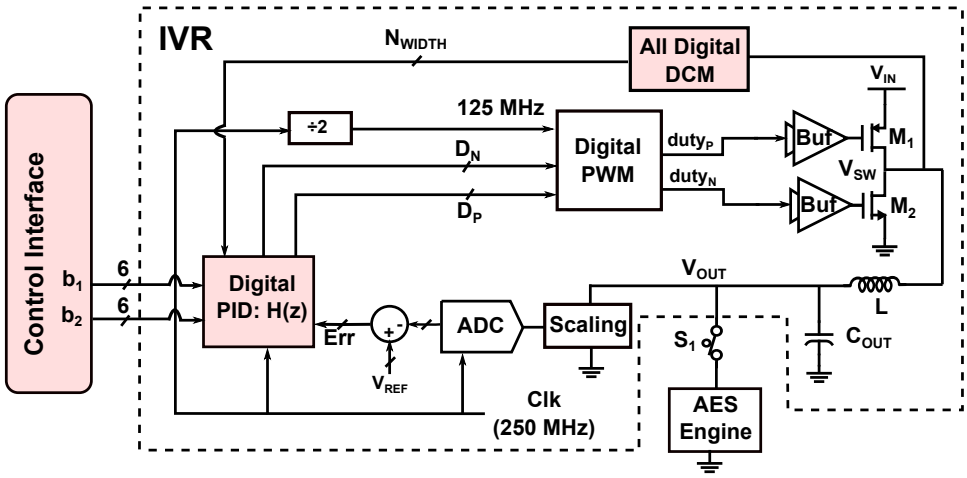

Figure 5.1: IVR Architecture with blocks affecting side channel resistance

Digital PID and PSCA resistance

The digital PID controller along with the small signal gain across the ADC and the DPWM determines the transfer function of the control path in the IVR. As demonstrated in Chapter 3, the small signal transfer function plays an important role in modifying the PSCA resistance. A control interface sets appropriate coefficients into the digital PID for modulating PSCA resistance.

DCM Engine and PSCA resistance

The DCM engine as elaborated in Chapter 4.4.3 (Fig. 5.2a) can improve IVRs power efficiency at low load current as the driving losses and conduction losses in the IVR become comparable to the output power. The negative inductor current sensor digitally senses the switch node (V_{SW}) and ensures that M_2 turns off exactly when the inductor current is zero. The DCM engine generates a 6-bit word N_{WIDTH} which represents the on-time of M_2. N_{WIDTH} is added to compensated and saturated error D_P to generate the off-time of M_2 (D_N). Subsequently D_P and D_N are fed to the DPWM engine as shown in Fig. 5.1. Figure 5.2b shows an example waveform of the I_L and the corresponding pulses driving M_1 and M_2. Whenever the digital sensor senses a zero or a positive I_L, N_{WIDTH} starts to incre-

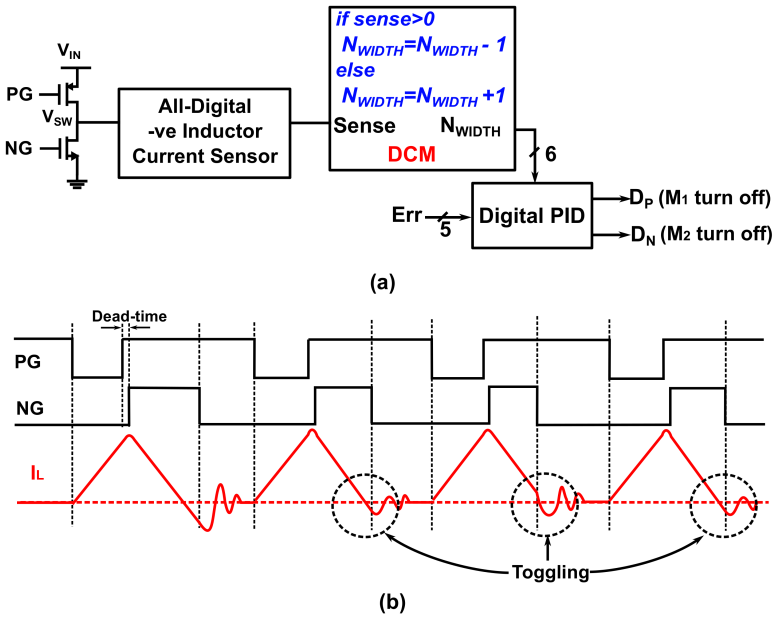

Figure 5.2: (a) All-Digital DCM Engine (b) Continuous toggling between two values of N_{WIDTH}

ment. As soon as I_L again becomes negative, N_{WIDTH} starts to decrease. The continuous toggling between the two values of N_{WIDTH} at a steady load current changes the large signal transformation as well as the misalignment effect, described in section 3.2.

5.1.1 AES Architecture

Two 128-bit AES architectures have been implemented in the test-chip and are described below.

1. **High-Performance AES (HP-AES)**: This architecture is suited for a high performance system where each AES round is executed in 1 cycle. The latency for one encryption is 11 cycles and all 16 bytes of the intermediate state are processed in the same cycle. Due to simultaneous processing of the intermediate states and on-the fly key generation, no intermediate storage is required. The architecture is shown in Fig. 5.3a.

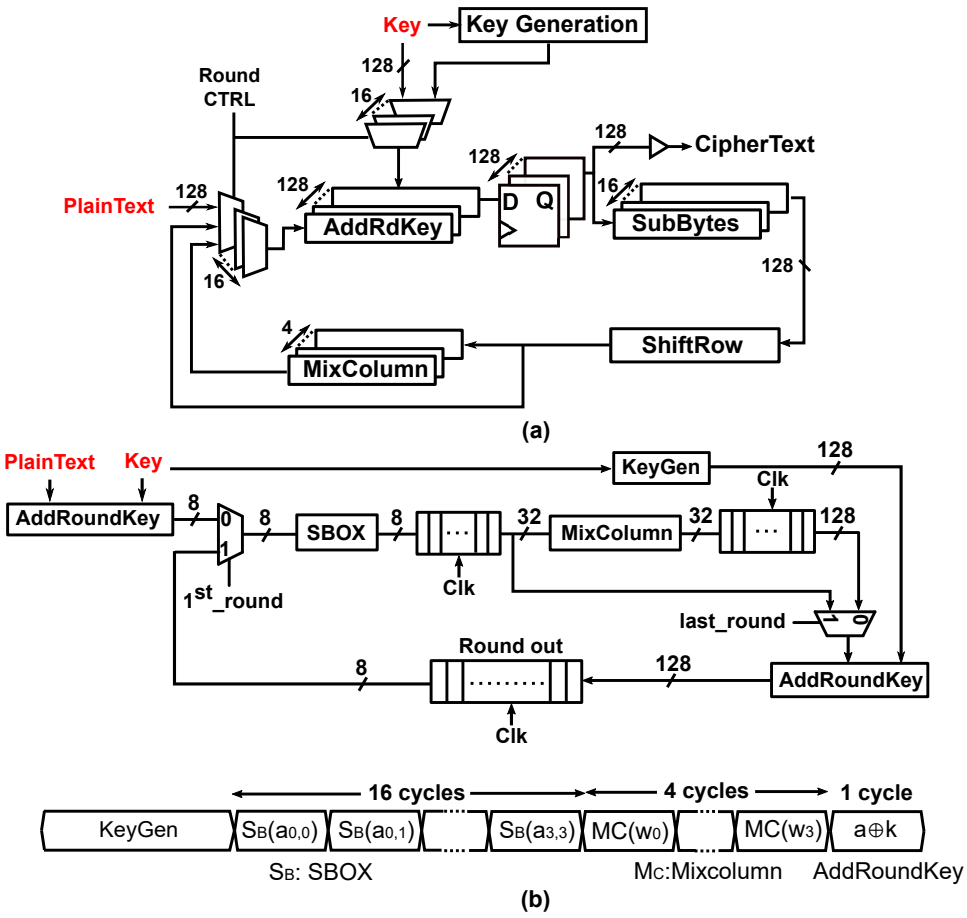

Figure 5.3: Architecture of the implemented AES engine (a) HP-AES (b) LP-AES

2. **Low-Power AES (LP-AES)**: This architecture, shown in Fig. 5.3b, is suited for a low-power, low-area application. The 8-bit datapath consists of a single S-BOX, 8 XORs for AddRoundKey, a byte-serial mix-column and intermediate registers for data storage. The latency for one encryption is 500 cycles.

5.2 Misalignment effect through an IVR

Successful key-extraction attacks exploit the correlation between the power consumption and the data processed in the underlying algorithm. The traditional statistical methods used in attacks like CPA or Differential Power Analysis (DPA) rely on the fact that the measured traces are aligned with respect to the rounds of the algorithm. This ensures that at a given

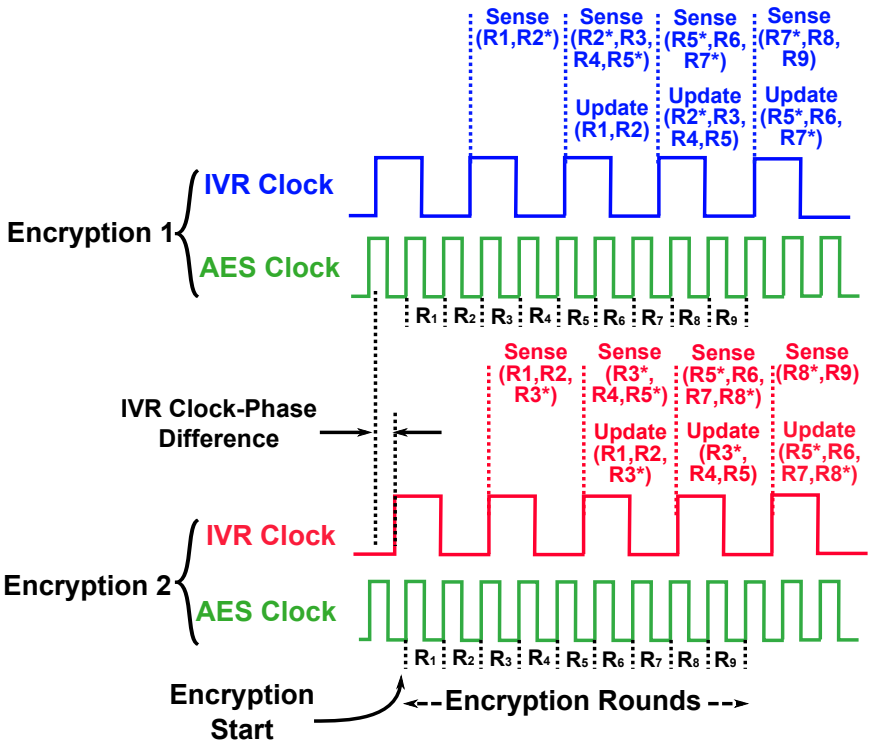

Figure 5.4: Misalignment effect in the captured input signatures due to asynchronous nature of the IVR_{CLK} and the AES_{CLK}

sample point in the measured traces, the same step of the algorithm is executed. For an IVR powered encryption engine, the encryption clock is asynchronous with respect to the IVR switching clock. The IVR switching clock is determined by factors like the values of the output filter passives as well as the number of IVR phases, whereas the digital clock is set by the throughput requirement.

Figure 5.4 shows the IVR clock and the encryption clock (AES_{CLK}) for two encryption events. Due to the asynchronous nature between the IVR_{CLK} and AES_{CLK}, each recorded traces will have different delay between the start of the encryption and the next IVR clock edge. We have denoted the rounds of the encryption engines are R_i. We note that the current signatures propagates directly to the IVR input through the IVR power stage when the transistor M_1 is on. The leakage through the control path is delayed by one cycle of the IVR_{CLK}. Figure 5.4 shows that the leakage through the control path depends on the relative

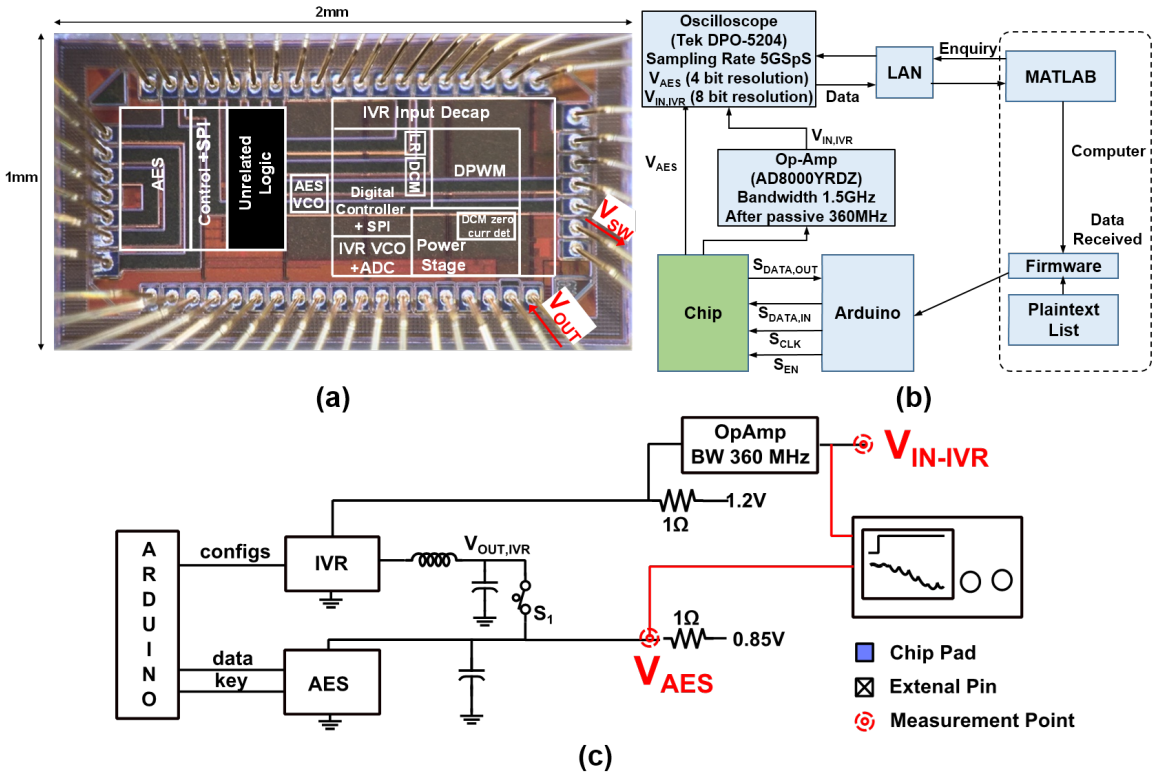

Figure 5.5: (a) Micrograph of the fabricated test-chip. Different blocks and their placements are shown (b) Test and firmware setup (c) Measurement points for PSCA

positioning of the IVR clock edges and the encryption rounds. If AES_{CLK} is faster than the IVR_{CLK}, multiple rounds of the encryption algorithm are mapped to one IVR duty cycle update. If AES_{CLK} is slower than the IVR_{CLK}, one encryption round is mapped across multiple duty cycle update. Moreover the relationship between the encryption rounds and the IVR phases are unique for each measured traces as shown in Figure 5.4. This misalignment effect helps to improve the PSCA resistance.

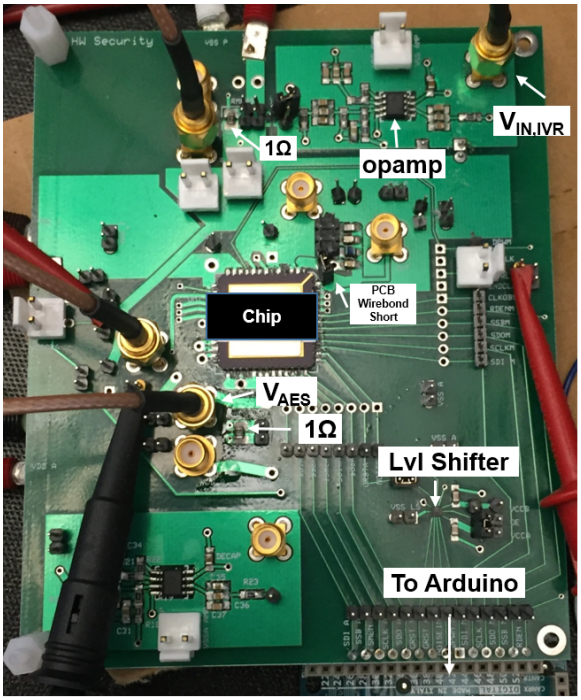

Figure 5.6: PCB for characterizing PSCA signature

5.3 Measurement Methodology

5.3.1 TestChip and PCB

The proposed architecture was fabricated in a 130nm CMOS technology. Fig. 5.5a shows the die photo. The IVR can convert 1.2V input to 0.45V-1V output. The control logic and other configurations are written in the IVR and the AES through two separate serial-to-parallel (SPI) interfaces.

Measurement Modes

To keep the provision of testing the AES engine separately, separate pads are created for the V_{DD} and V_{SS} of the AES engine. Side channel signatures are measured for the following conditions.

1. **Standalone AES**: The AES is powered through the dedicated V_{DD} and V_{SS} pins of the AES engine. Switch S_1 in Fig. 5.1 is kept open. The AES is supplied at 1.2V and

operates at 40MHz clock. In this mode, the signatures at the V_{AES} node is measured.

2. **Baseline IVR-AES**: Switch S_1 is closed and the IVR output is set at 0.85V. The IVR drives a high load current created through a synthetic load generator and therefore remains in continuous conduction mode (CCM). In this mode, the signatures at both V_{AES} and $V_{IN,IVR}$ nodes are measured. We note that in practice, the local AES supply node (V_{AES}) won't be accessible to the adversary. However, for a pessimistic security analysis, we measure V_{AES} signatures and exploit them for post-processing and alignment as will be shown in section 5.4.1.

3. **IVR-AES in DCM**: The IVR output is set at 0.85V, however the synthetic load generator is turned off. The IVR goes into DCM.

Measurement environment

Fig. 5.5b shows the corresponding PCB for PSCA measurements. A 1Ω resistor is inserted in the series path of the AES supply (for standalone AES measurements) and the IVR supply (for IVR-AES measurements). A 360MHz bandwidth low-noise amplifier is used to amplify the IVR input signatures.

5.3.2 Statistical Tests

Correlation power Attack

CPA, explained in chapter 3.5.2, is used to quantify the PSCA resistance of both the standalone AES as well as the IVR-AES. For HP-AES, the hamming distance across the 1st round SBOX which is a commonly used power-model, might not be effective, as the transition times of the output bits of the SBOX are different. Therefore, the hamming distance between the intermediate state (128-bit) at penultimate round and the last round of the encryption (intermediate state of last round is also the ciphertext) is used as a power-model for CPA. The power-model captures the power consumption of register shown in Fig. 5.3, in

particular the 8 flipflops associated with the corresponding key-byte. The LP-AES power-model is elaborated in section 5.4.2.

Test Vector Leakage Assessment

The success of a CPA is critical on the choice of the power-model. Although a successful CPA is clearly an indication of design vulnerability to a PSCA, an unsuccessful CPA does not guarantee that the underlying platform is not leaking, particularly from a designer's point of view. A rigorous process involving security analyses with different power-models might be carried out at the cost of high testing time, however, no conclusive results might be obtained about the vulnerability of the targeted platform. Test Vector Leakage Assessment (TVLA) as proposed by Goodwill et. al in [98], is a testing methodology which does not aim at recovering secret keys from the underlying encryption engine, rather finds out whether the side channel signatures are correlated to the internal power consumption.

In TVLA a tester encrypts two plaintext lists PT_1 and PT_2, ($|PT_1| = |PT_2| = n$) with a known key K_T. PT_1 consists of statistically random inputs. PT_2 consists of either a same input PT' (fixed TVLA dataset) or a set of key-specific unique inputs (semi-fixed TVLA dataset). An AES encryption with any plaintext from the second list and key K_T satisfies a set of criteria, listed in [98], ensuring that one of the chosen intermediate AES rounds (R) shows minimum leakage. The measured dataset $[M]_{n\times T}$ is split into two partitions $[M_1]_{n\times T}$ and $[M_2]_{n\times T}$ according to the plaintext list. A Welch's T-test is performed between the two lists.

$$t - val_t = \frac{\mu_{M_1} - \mu_{M_2}}{\frac{s_{M_1^2}}{n} + \frac{s_{M_2^2}}{n}}, 1 \leq t \leq T \tag{5.1}$$

A high t-value at a certain time instant indicates that the two partitions are statistically distinguishable, which further implies that the power consumption of the target device during computation of the chosen round R is correlated with the underlying data. A t-value of more than 4.5 for n$\geq$5000 has 99.9999$\%$ probability that the underlying device is leaking. Multiple works have reported that TVLA is a more powerful statistical analysis than CPA

and therefore is used in cases whether we were not able to mount a successful CPA.

5.4 Results

The measurement methodology is shown in Fig. 5.5c. PSCA signatures are captured with 5GSps sampling with 8 bit resolution over the oscilloscope window. The following discussion details PSCA resistance of both AES architectures, in operating modes described in section 5.3.1.

5.4.1 HP-AES

Sample waveforms

We first start with characterizing the standalone-AES (5.3.1). Fig. 5.7a shows the signature on V_{AES} when the AES is powered externally along with the corresponding AES clock. As the AES is implemented using an unprotected CMOS logic family without any architectural or algorithmic countermeasures, it is easy to figure out the 11 round operation of the AES. Next the AES is supplied by the IVR in CCM mode (5.3.1). Fig. 5.7b shows the signature on $V_{IN,IVR}$ during an AES encryption. We point to few interesting observations from the $V_{IN,IVR}$ signature as well as its FFT shown in Fig. 5.7c.

- The dominant component in the $V_{IN,IVR}$ signature is the IVR_{CLK} and its higher harmonics. The 3rd harmonic shows in the highest spectral content.
- The AES rounds are not visible in the $V_{IN,IVR}$ signature. Therefore, if V_{AES} is physically inaccessible to the adversary (which generally is the case for a practical system), identifying the AES portion from the $V_{IN,IVR}$ signature would be difficult.

Next the IVR load current is reduced to force the IVR into a DCM mode. Fig. 5.8a shows $V_{IN,IVR}$ signature when the IVR enters into a DCM mode. As a result of continuous toggling of the pulse width of M_2 which is similar to a limit-cycling effect, the current

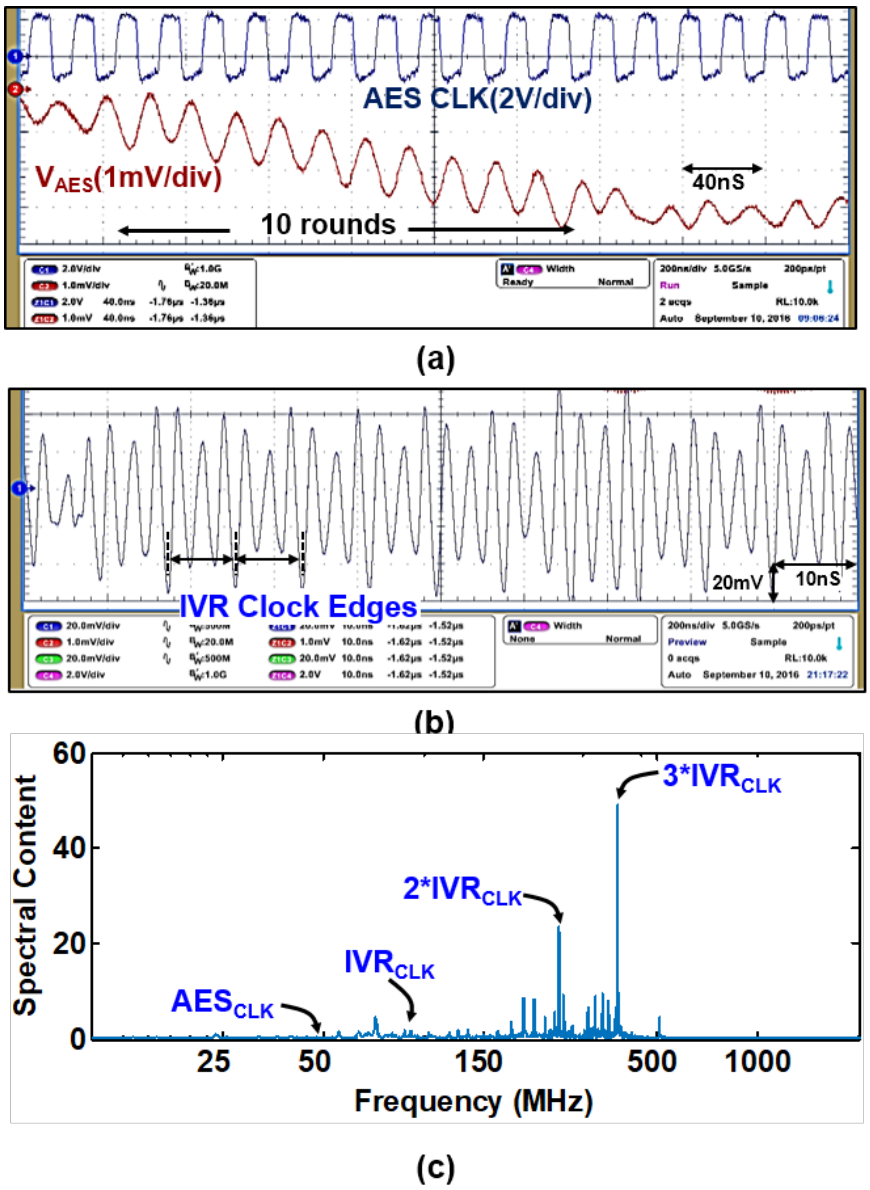

Figure 5.7: (a) PSCA Signatures of a Standalone AES captured at V_{AES} (b) PSCA Signatures of a IVR-AES captured at $V_{IN,IVR}$ (c) FFT of $V_{IN,IVR}$ signature

transformation through the IVR is changed.

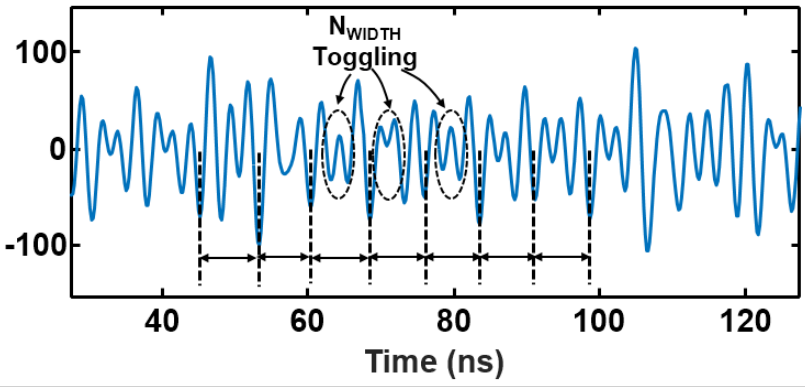

Figure 5.8: (a)$V_{IN,IVR}$ signature when the IVR is in DCM mode

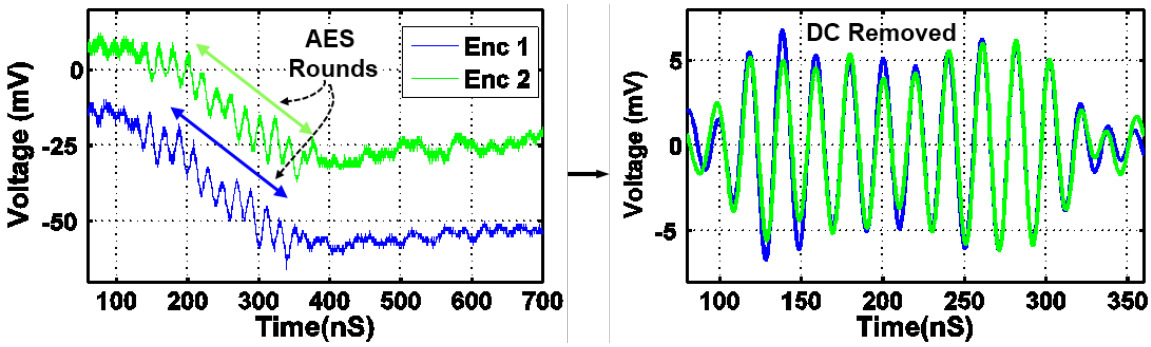

Figure 5.9: V_{AES} signatures for two encryption events before and after alignment

Post-Processing and Alignment

The alignment of the measured traces is critical for performing a key-extraction attack through CPA or characterizing the information leakage through TVLA. The trigger used in the measurement setup (Fig 5.5c) is not synchronous with respect to both the IVR_{CLK} and the AES_{CLK}, therefore alignment is extremely critical for the designed prototype. As AES rounds are clearly visible in the V_{AES} signature, irrespective of whether it is supplied by an external source (standalone AES) or the IVR, the V_{AES} signatures are first filtered at the AES_{CLK} frequency and the filtered signatures are aligned with respect to cross correlation (Fig. 5.9).

Aligning $V_{IN,IVR}$, through the same method might not be useful as the IVR_{CLK} is at a

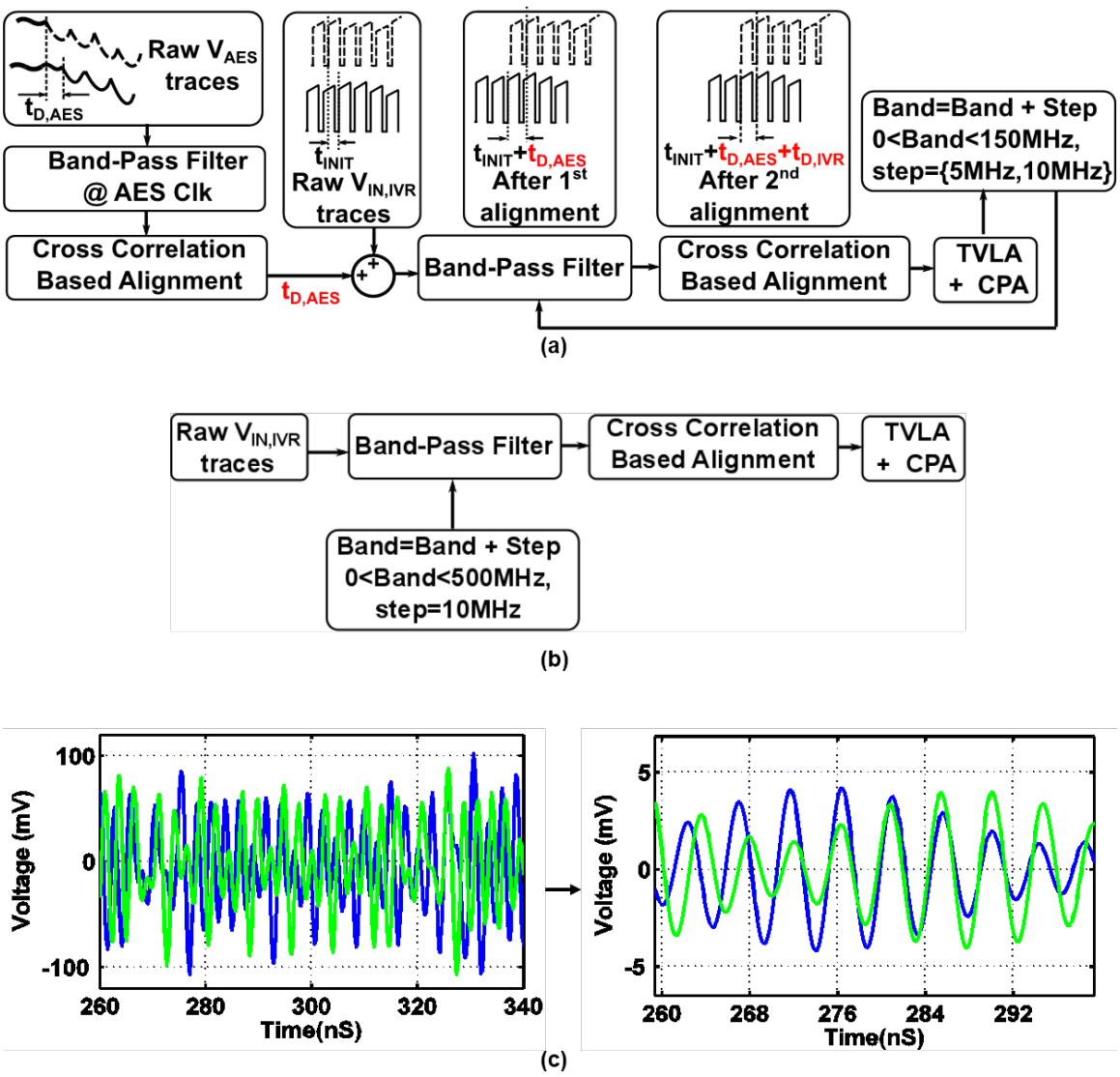

Figure 5.10: (a) Two step alignment of $V_{IN,IVR}$ using V_{AES} (b) Single step alignment of $V_{IN,IVR}$ (c) $V_{IN,IVR}$ signatures for two encryption events before and after alignment

higher frequency than the AES_{CLK}, therefore the information of a particular AES round for two recorded traces might be apart by more than one IVR cycle. Therefore a direct cross-correlation is not guaranteed to align the $V_{IN,IVR}$ traces with respect to the same round of the AES. Two alignment approaches are initially tried and the details are explained below (Fig 5.10).

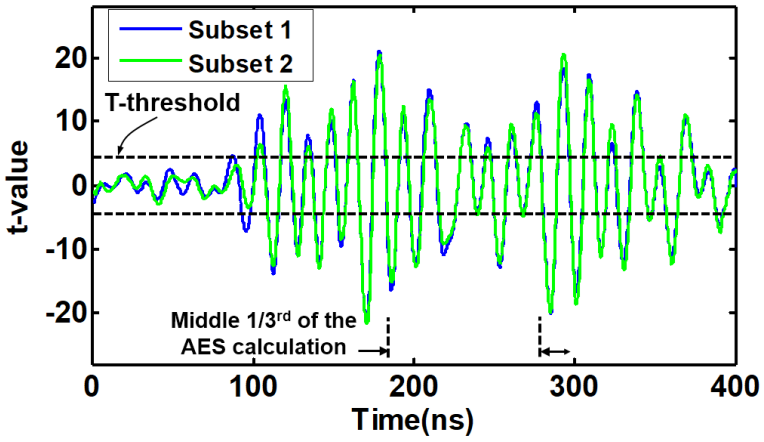

Figure 5.11: TVLA on a standalone AES

Two step alignment using with V_{AES}: We assume a pessimistic scenario where the adversary has access to V_{AES} as well. A series of bandpass filters, with center frequencies varying from 5MHz to 150MHz in steps of 5MHz are used to filter the $V_{IN,IVR}$ signatures. The filtered signatures are first offset by the offset time obtained from the alignment process of the corresponding V_{AES} signature. This ensures that the IVR clock phase containing the information of a particular AES round is separated by a maximum time delay of one IVR cycle and therefore a cross correlation is used to align the waveforms. We note that the maximum offset during cross correlation is limited by the corresponding filter band.

Alignment without V_{AES}: Here we assume that the adversary does not have access to V_{AES} and a similar methodology for aligning V_{AES} in a standalone mode is adopted. A series of bandpass filters, with center frequencies varying from 10MHz to 500MHz in steps of 10MHz are used to filter the $V_{IN,IVR}$ signatures and the filtered signatures are aligned using cross-correlation, with the correlation offset bounded by the filtering frequency. A wider frequency range is used for filtering in this alignment method, as it will be evident in the next section.

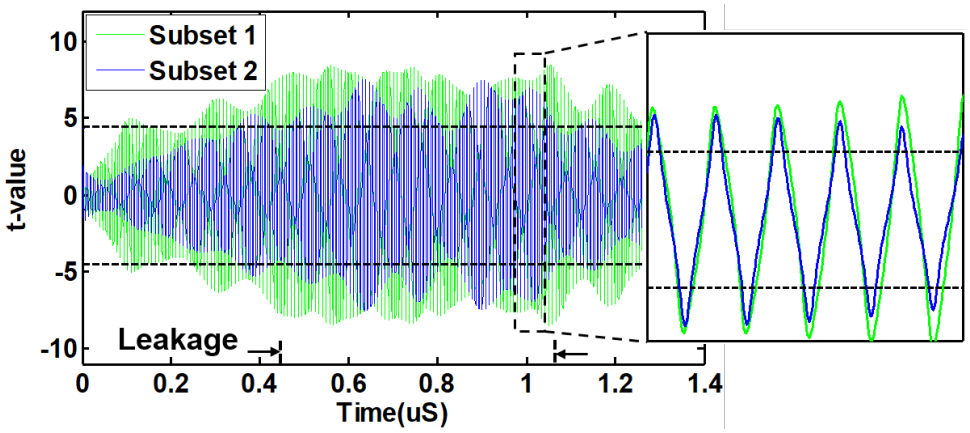

Figure 5.12: TVLA for baseline IVR in CCM mode, post-processed at 125MHz frequency

TVLA

TVLA is performed with 5000 plaintexts (fixed dataset, total 10000 encryptions) in each set PT_1 and PT_2 ($n = 5000$), unless otherwise mentioned. We first start with performing a TVLA on the standalone AES. Fig. 5.11 shows the t-value against time for two experiments. The t-value crossed the 4.5 threshold at multiple time instants and is consistent for multiple experiments, clearly indicating leakage. For a fixed dataset, as the same plain-text is selected every time from PT_2, the power consumption during load and store as well as other intermediate rounds can lead to peaks in t-values. However, these peaks are counted as false peaks as the goal is to observe data dependent leakage from the computation of the intermediate rounds. Therefore, the peaks in the middle one-third of the encryption corresponds to information leakage generated from intermediate AES rounds, as demarcated in Fig. 5.11.

Baseline IVR:For the baseline IVR in CCM mode, no successful TVLA was observed before any alignment (sec 5.4.1). Fig 5.12a shows TVLA results on post-processed $V_{IN,IVR}$ signatures at a 125MHz frequency band, using the first post-processing technique. We note the following interesting observations

- The t-value profile against time are different for different experiments. However, as

marked in Fig. 5.12, both the experiments show a t-value of more than 4.5 from 0.4μs to 1μs which indicates with sufficient confidence that there is information leakage.

- The t-value above the 4.5 threshold is spread across multiple peaks in the post-processed signal. As IVR_{CLK} is higher in frequency than the AES_{CLK}, information of one AES round is spread in multiple IVR clock phases. Moreover, filtering the $V_{IN,IVR}$ signatures causes further spreading of leakage.

- The peaks due to load/store of the plain-text/cipher-text and the same due to intermediate rounds are indistinguishable. This again creates a pessimistic evaluation scenario as the leakage seen in the baseline IVR might be only due to load/store.

TVLA across different frequency band

Fig. 5.13 shows the peak t-value against frequency (center frequency of the filter band used for post-processing) for the two techniques described in section 5.4.1. Each plot contains TVLA results for the baseline PID configuration and two other configurations where different zero locations are used in the PID. The transfer function of the PID compensator changes the small signal transformation through the IVR as described in section 3.2. We note the following observations:

- Both alignment techniques show TVLA leakage. This result is interesting as it suggests that a AES_{CLK} agnostic alignment can exploit the $V_{IN,IVR}$ signatures.

- There are distinct frequency bands that leak information for all zero locations. These bands remain fixed across different zero locations in the PID controller. For the first alignment method, the probable reason of leakage from the 50MHz to 70MHz band is due to its proximity to the AES frequency (40MHz) as well as the package resonance frequency (65-70MHz)and the leakage from 120MHz to 130MHz band is due to the IVR_{CLK} (125MHz). For the second alignment method, no TVLA leakage is observed from 0-200MHz. However, frequency bands beyond 200MHz shows leakage. The

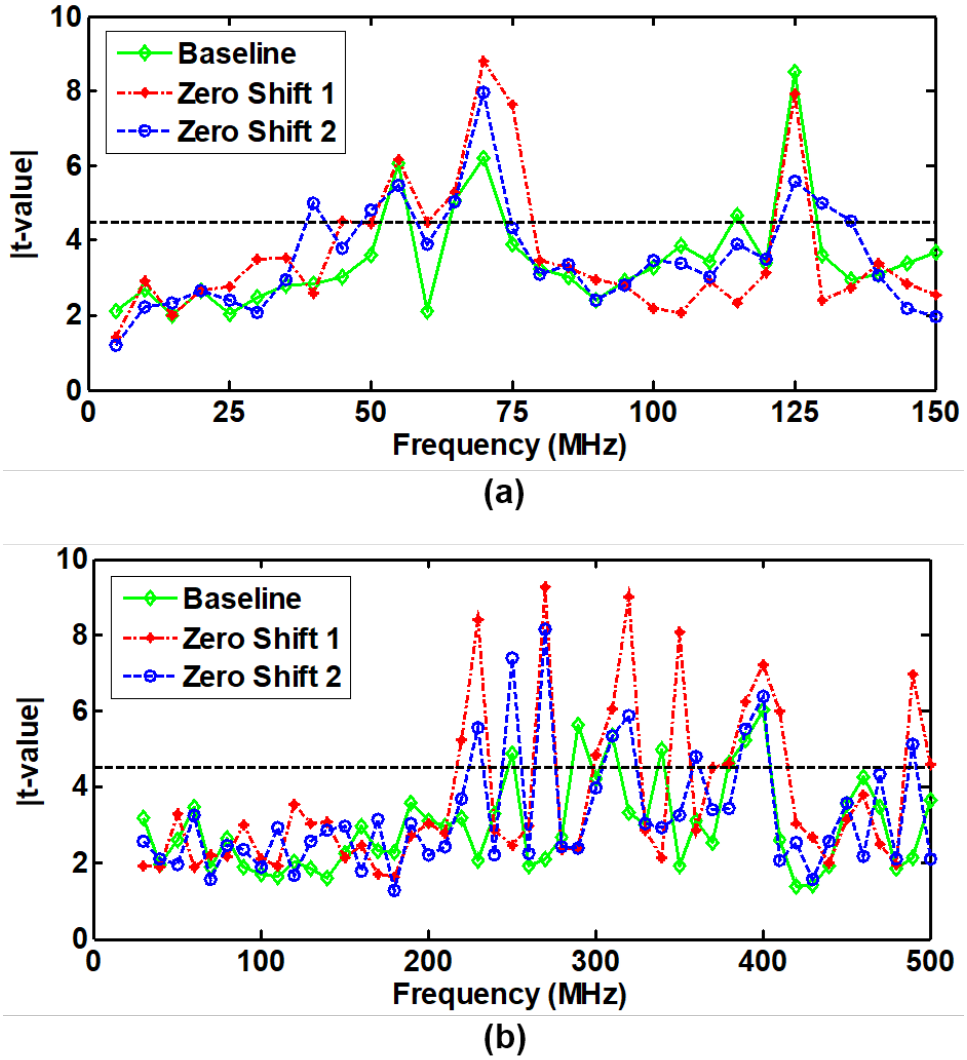

Figure 5.13: TVLA results on baseline IVR against frequency bands used for filtering $V_{IN,IVR}$ signatures (a) Alignment using V_{AES}, 10000 traces (b) Alignment without V_{AES}, 70000 traces

possible explanation of this behavior is the side channel signatures from one AES_{CLK} cycle are coupled to multiple cycles of $V_{IN,IVR}$ and its harmonics. Therefore, even if the origin of the signature from the AES engine are time-shifted (maximum shift is bounded by $1/AES_{CLK}$), the data-dependency at the $V_{IN,IVR}$ signature is independent of this time shift. The results also show that a wider frequency range needs to be used to identify the leakage if the second alignment process is used.

Table 5.1: Performance Trade-off

IVR-AES Design Settings	Max t-value	Droop (mV)	Settling time (ns)
Baseline	8.49	84	80
Zero Loc 1	8.825	86	82
Zero Loc 2	7.97	96	95

- The peak t-value at different frequency bands change as the PID zero locations change. This is expected as changing zero locations change the small signal transformation which controls the leakage (peak t-value at a certain frequency band).

- Performance trade-off: The shift in the peak-t-values for different zero locations suggest that the compensator transfer function can be potentially used as a control knob to alter PSCA resistance. The modified zero locations maintain stability of the IVR, however, the response to load and reference transient change. Table 5.1 shows the droop and the settling time to a 0-55mA droop (created by an on-chip synthetic load current generator) for the selected set of coefficients.

We used the second alignment technique for further results as it is equally effective in identifying leakage and independent of any assumption about observability of V_{AES}.

DCM: One of the prevalent techniques in improving the signal to noise (SNR) ratio of all forms of side channel measurements is to shut off other modules in the processor other than the encryption engine. This is easy to achieve as the adversary can simply wait to start the side channel measurement once the other system activities are reduced. If an IVR is used to supply the processor along with the AES engine, the reduction in load current supplied by the IVR will force the IVR into a DCM mode. The inductor ripple current for the designed IVR at a 0.85V output is 110mA. Therefore, if the total load current drawn from the IVR reduces below 55mA, the IVR would move into a DCM mode. The designed AES engine at a 0.85V supply 40MHz frequency draws $<$10mA current ensuring the previous condition if the AES is the only load to the IVR. Fig. 5.14 shows that the

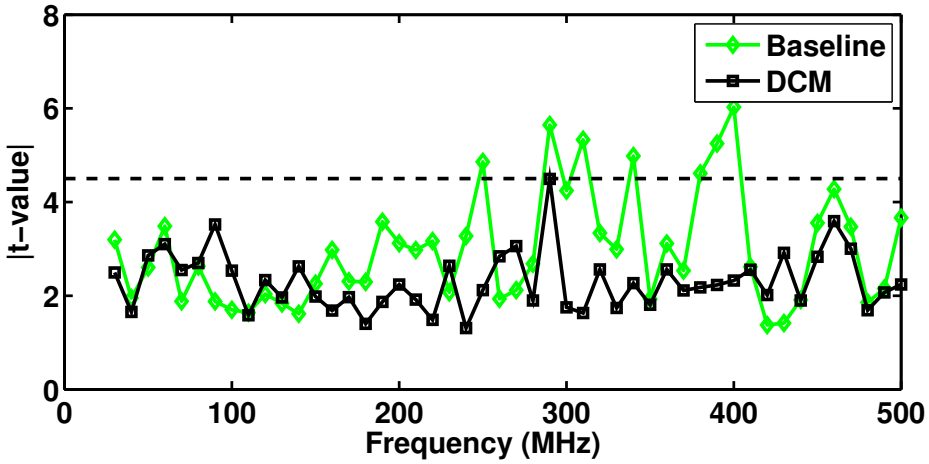

Figure 5.14: TVLA results for the IVR in a DCM mode (alignment without V_{AES}, 70000 traces)

peak t-value remains below the 4.5 threshold when DCM is enabled and therefore prevents information leakage irrespective of a higher SNR of measurement.

CPA

A leakage test like TVLA indicates that there is a data dependency in the measured side channel signature. However the ultimate purpose of a side channel attack is to extract the key from the underlying device. To demonstrate the improvement in PSCA resistance for a key-extraction attack, we performed a CPA on the standalone AES as well as on different configurations of the IVR-AES system. As the last round does not have a mix-column step, the hamming distance can be calculated per key-byte basis assuming that the adversary can observe the ciphertext.

Standalone AES: The standalone AES is implemented in unprotected static CMOS and is vulnerable to CPA with the chosen power model. The V_{AES} signatures have been filtered and aligned as discussed as described in section 5.4.1. Fig. 5.15a shows the correlation against time for all possible 256 guesses of the 10th key byte, with the correct key byte marked in black. The correlation of the correct key attains the maximum absolute value compared to the same for the incorrect keys and therefore can easily be distinguished. Fig.

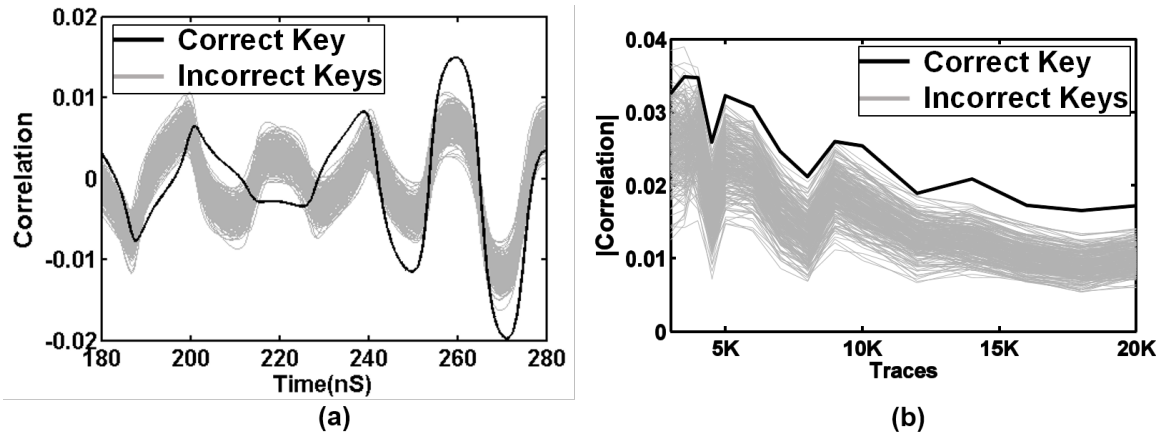

Figure 5.15: CPA on V_{AES} for a Standalone AES configuration (a) correlation vs. time (b) correlation vs. traces

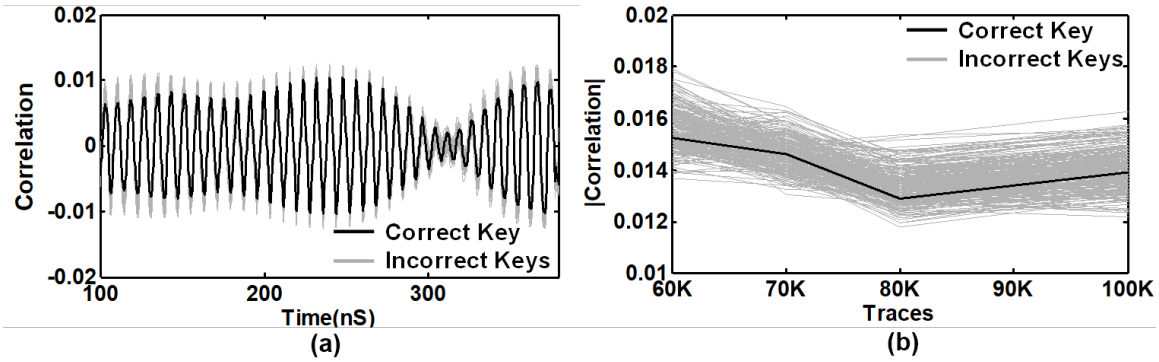

Figure 5.16: CPA on $V_{IN,IVR}$ signatures for a baseline IVR-AES configuration (a) correlation vs. time (b) correlation vs. traces

5.15b shows the maximum correlation against a number of traces used for correlation. 5000 traces are enough to correctly identify the 10th key byte.

IVR-AES: We first start with performing CPA on the baseline-IVR design. Although TVLA shows leakage across multiple filter bands, no successful CPA was observed across all these bands with the second alignment technique. For TVLA, a slice of 200ns from the $V_{IN,IVR}$ signatures was used in computation. However, for a successful CPA, alignment is

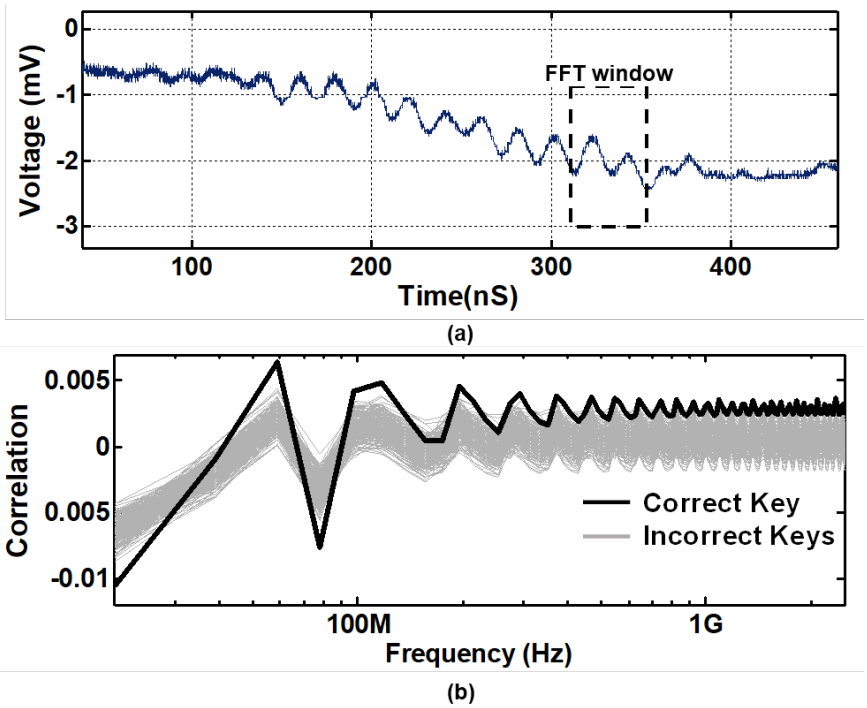

Figure 5.17: Frequency domain CPA on standalone AES (a) selection of window for FFT (b) correlation vs. frequency for all key guesses

more critical as the power consumption of the targeted register has to be exactly aligned. We used a slice of 20ns sliding it across a region of 200ns in steps of 10ns, post processed each of these slices and performed a CPA. Fig. 5.16 shows correlation against time (across all slices and all frequency bands) for the baseline IVR-AES and it is not possible to find out the correct key. Fig. 5.16b shows peak correlation against traces. The results clearly indicate that 100,000 traces are not enough to find out the correct key. This is an interesting observation as the baseline IVR configuration without any power, performance and area overhead can improve PSCA (CPA) resistance by $\geq$20x.

Frequency Domain CPA: One of the possible reasons, a hamming distance based power model might fail in CPA is random shift of the information content in time domain due to misalignment present in the baseline IVR, explained in Chapter 5.2. Time-shift based desynchronization has been a popular countermeasure for PSCA, where NOPs (no-operations) are inserted randomly in the intermediate steps of an encryption algorithm

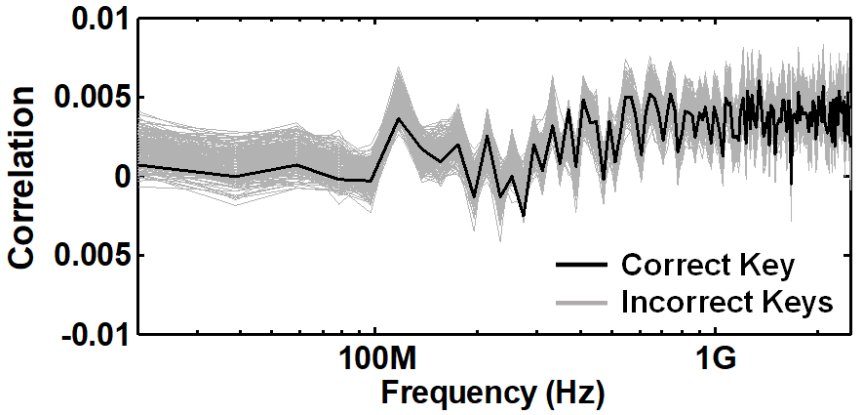

Figure 5.18: Frequency domain CPA on baseline IVR-AES

[27]. Frequency domain attacks can successfully break such countermeasures as frequency domain representation (FFT, Spectrogram, DWT) of a signal decouples the magnitude and phase information and therefore the time-shift does not affect the data dependency in the magnitude information. One other advantage of a frequency domain CPA is that the same power-model can be used for attack as magnitude in frequency domain is proportional to magnitude in time-domain and no signal post-processing is necessary.

One of the drawbacks of a frequency domain CPA is the difficulty in accurately capturing the region of interest. Typically only a small section of the measured waveform contains the exploitable signature. Therefore, performing an FFT over the entire trace causes *dilution* of the signature with noise. A window with appropriate length, small enough so that signatures of interest are captured and large enough so that the exploitable signature remains within the chosen window, even after worst case time-shift, needs to be chosen.

For the following results, we have chosen a window of 40ns to perform a frequency domain CPA. Fig 5.17 shows the window selection and the correlation against frequency for all the key guesses. It can be clearly seen that the correct key can be identified.

For $V_{IN,IVR}$ signatures, the same window length is assumed as the maximum shift in time is limited by $\frac{1}{AES_{CLK}} + \frac{1}{IVR_{CLK}} 0 \leq 40ns$. Fig. 5.18 shows the frequency domain CPA results on the baseline IVR-AES signatures. As evident, no successful CPA was observed.

Reversibility Attack Based on the RTF and the estimation procedure proposed in section 3.7.2, the $V_{IN,IVR}$ signatures are used to estimate the corresponding load current signatures at the IVR output. Simulation framework based results, shown in section 3.7.2 did not observe any additional advantage in using this threat model. However the information leakage behavior was consistent before and after applying the RTF i.e. the designs which showed a successful PSCA showed the same behavior after estimation. However, RTF performs poorly on the measured data as no TVLA leakage was observed after applying RTF on the $V_{IN,IVR}$ signatures in the baseline IVR configuration. Similarly, no successful TVLA was observed on the IVR configuration with different zero locations (the RTF sis modified accordingly) and DCM mode. The peak t-values after applying RTA on different IVR modes are shown in table 5.2.

Table 5.2: Maximum t-value after reversibility

IVR-AES Design Settings	Baseline	Zero Loc 1	Zero Loc 2	DCM
Max t-val after RTF	3.53	2.28	3.73	3.60

5.4.2 LP-AES

In this section, we present improvement in PSCA resistance for the LP-AES architecture. Result corresponding to the standalone AES and the baseline IVR-AES system are shown for brevity.

Sample Waveforms and Post-Processing

The side-channel-signature of the LP-AES is shown in Fig. 5.19. The figure shows the signature captured at the V_{AES} node in a standalone mode. As the computation is serialized and spread over a large number of clock cycles, the variation in V_{AES} is significantly smaller than a HP-AES, where the 10 round operation of the AES is clearly visible. The rounds of the AES are not distinct in the captured signatures. However, if the V_{AES} signature is

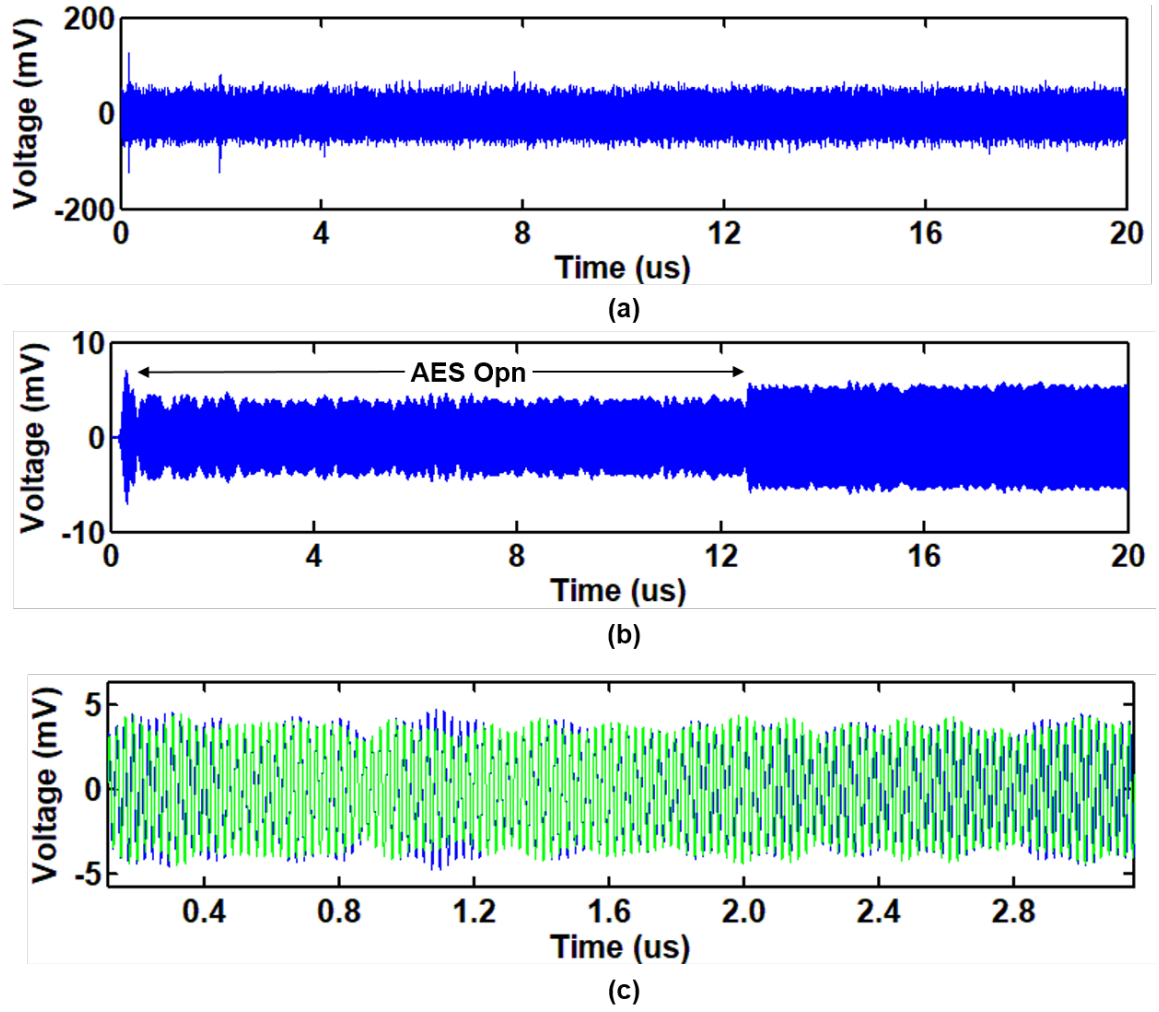

Figure 5.19: (a) V_{AES} in standalone configuration (b) V_{AES} after filtering using a 70MHz-90MHz bandpass filter(c) Aligned V_{AES} for two encryption events

filtered using a bandpass filter from 70MHz-90MHz, two distinct regions appear in filtered waveform. The LP-AES takes ∼500 clock cycles for one encryption, which translates to a 12.5us for a 40MHz clock frequency and can be identified from the filtered waveform. The $V_{IN,IVR}$ waveforms for a LP-AES look similar to the HP-AES and is not shown for brevity. This clearly suggests that the variation in current due to the AES operation for both architectures are small enough to create any visible difference in the $V_{IN,IVR}$ signature. Similar alignment process as described in 5.4.1 is used to align both V_{AES} and $V_{IN,IVR}$ signatures. Alignment of $V_{IN,IVR}$ does not include any offset from aligning V_{AES}.

TVLA

TVLA on the LP-AES are performed with a semi-fixed dataset. The required 4 criteria which each unique plain-text in the second dataset has to satisfy are satisfied individually by 4 bytes in the intermediate state at the end of the 4th round. As bytes are processed serially in the LP-AES, the TVLA criteria ensure minimum leakage across four clock cycles (corresponding to the four bytes which satisfies the conditions) which is enough for a TVLA test.

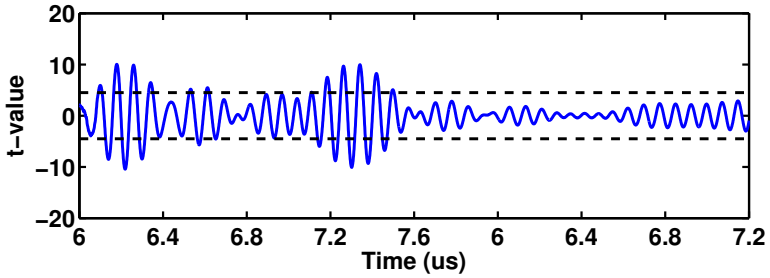

Figure 5.20: TVLA on V_{AES} for LP-AES in standalone mode

Standalone-AES: Fig. 5.20 shows TVLA on V_{AES} in the standalone mode. As the AES is implemented without any countermeasures, TVLA clearly shows signs of leakage.

Baseline IVR-AES: Fig. 5.21a shows TVLA results for baseline-IVR with LP-AES. Coherent with the result for HP-AES, the TVLA shows leakage. Approximately 2000

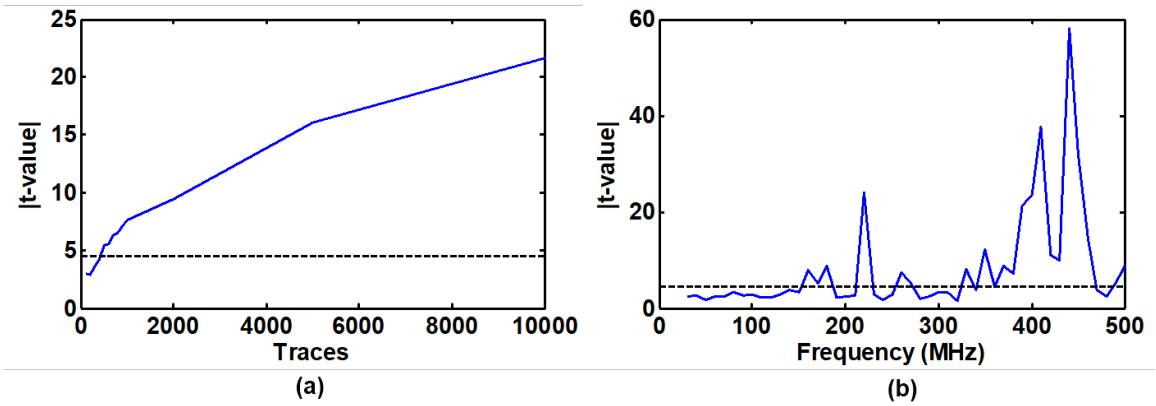

Figure 5.21: TVLA on $V_{IN,IVR}$ with Baseline IVR-AES (a) t-value against traces (b) t-value against frequency for 100,000 traces

traces are enough to achieve a t-value more than 4.5. Fig. 5.21b shows that the frequency components between 350MHz-500MHz band shows strong leakage. The leaking frequency bands for a V_{AES} independent alignment are coherent with HP-AES results shown in Fig. 5.13b.

CPA

CPA on LP-AES is carried out with the same plain-text list as HP-AES, however a different power-model is used. Using hamming distance across a register is more effective than hamming distance across a combinational block as outputs of a register transition in close proximity whereas outputs for a combinational block will have different transition times. As evident from Fig. 5.3, the individual bytes are executed serially in the LP-AES and the intermediate data are registered. The hamming distance across the S-BOX in the first round is chosen as power-model.

Standalone AES: Fig. 5.22 shows CPA on V_{AES} in a standalone mode. Fig. 5.22a shows that only 1000 traces are enough to extract the first key-byte using a CPA. When compared to the HP-AES, LP-AES turns out to be $\sim$5x less resistant to a CPA attack. This

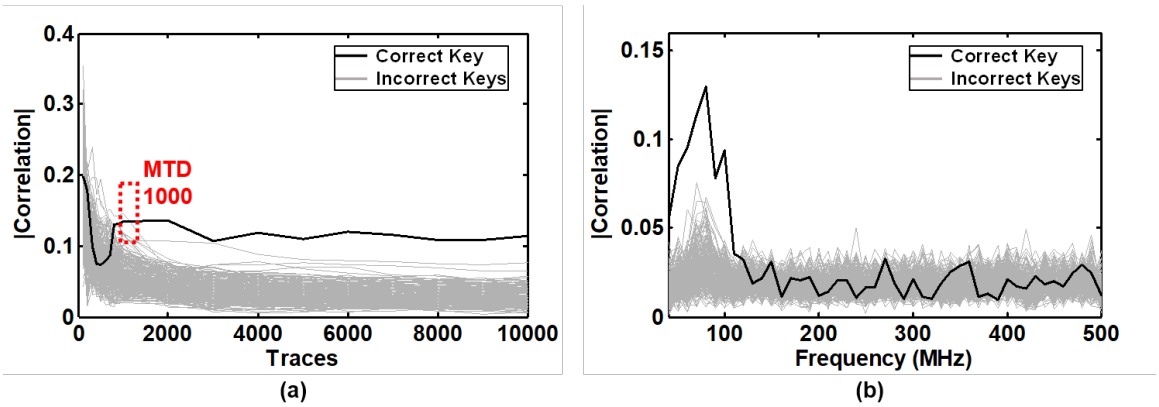

Figure 5.22: CPA on V_{AES} in standalone mode (a) peak correlation vs. traces (b) peak correlation vs. filter frequency

can be explained due to the serial nature of the computation. For a HP-AES the power-model is expected to correlate to power consumption of 8 flipflops, storing the corresponding byte. However, as the intermediate states is 128-bit wide, the power consumption of rest 120 flipflops act as noise. In LP-AES, at a given time instant, the state of only 8-bit flipflops are changing as the datapath is 8-bit wide. Therefore the power consumption correlates perfectly with the power-model. This shows that LP-AES or any AES with a serialized datapath is more vulnerable to key-extraction attacks.

Fig. 5.22b shows the peak correlation for all key-guesses against frequency band. As the AES operating frequency was 40MHz, frequency bands from 20-100MHz, which covers the AES_{CLK} and the second harmonic, shows a successful CPA.

Baseline IVR-AES: For the HP-AES, the baseline IVR, although showed a successful TVLA, didn't show a successful CPA. However, for the LP-AES the baseline IVR shows a strong CPA, as shown in Fig. 5.23a. 1500 traces are enough to extract one of the key-bytes, merely improving the CPA by 1.5x compared to the standalone AES. This is a significant result as it shows that a successful CPA can be performed on $V_{IN,IVR}$ with the same power-model used for the standalone AES. The reason behind this observation is explained in

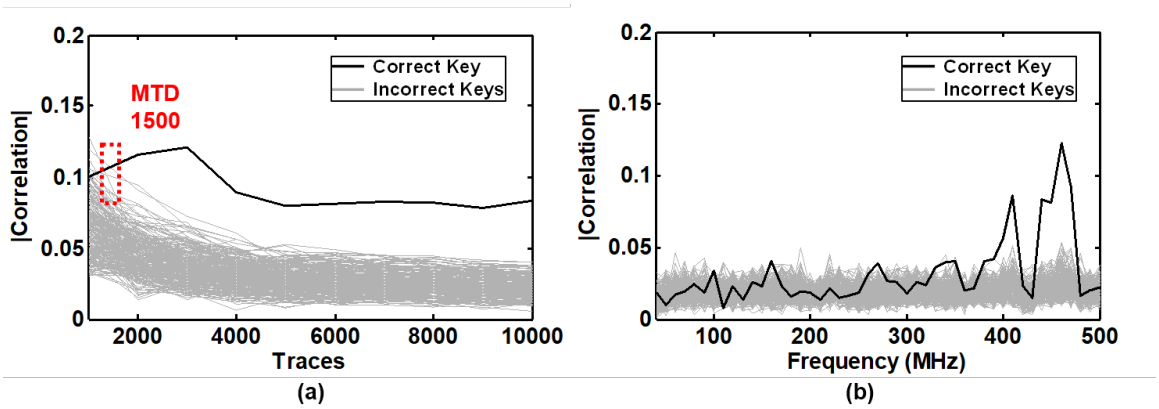

Figure 5.23: CPA on $V_{IN,IVR}$ for the baseline-IVR (a) peak correlation vs. traces (b) peak correlation vs. filter frequency

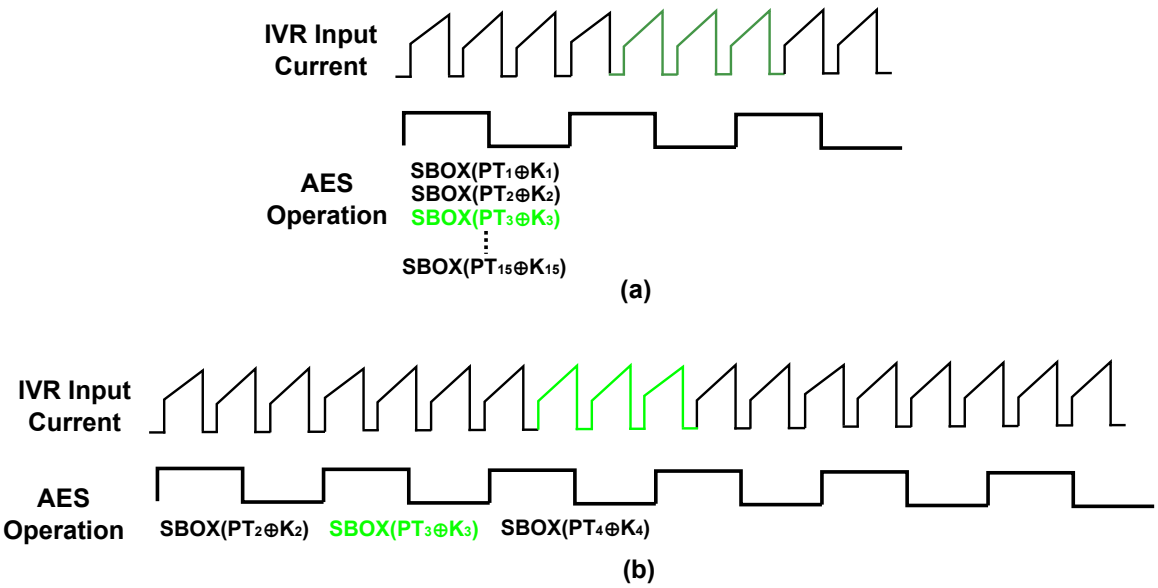

Figure 5.24: Side channel leakage at IVR input for (a) parallel vs. (b) serial operations of the AES intermediate steps

Fig. 5.24. As the AES_{CLK} frequency for the test condition is almost three times slower than the IVR_{CLK}, information corresponding to processing of one byte, assuming a serialized operation of the AES (LP-AES), is spread across three IVR cycles. As explained earlier, a serialized operation shows a good correlation between power-model and power consumption. Even if the $V_{IN,IVR}$ signatures are not aligned with respect to the AES_{CLK}, aligning $V_{IN,IVR}$ with respect to IVR_{CLK} and its higher harmonics ensure that at-least one IVR cycle (marked green in Fig. 5.24) will for all the traces will overlap. The PSCA resistance at the IVR input can potentially improve if a higher AES_{CLK} frequency is used.

5.5 Summary

The PSCA resistance of a baseline IVR, i.e. an IVR architecture without any security aware design, is characterized through measurement results for two architectures of a 128-bit AES. For the HP-AES design, which in a standalone configuration shows a successful CPA with 5000 measurements, didn't show any successful CPA at IVR's input with 100,000 traces. The LP-AES design, where the execution is byte-serial has a standalone MTD of 1000 and shows that serialized designs are more vulnerable to CPA. A successful CPA was observed at the IVR's input for the LP-AES design, with only 1500 measurements using the same power-model. TVLA shows information leakage at IVR input in CCM mode for both HP-AES and LP-AES. This indicates that depending on the architecture of the AES implementation, a baseline IVR design *can be used* for improving resistance against CPA, though a baseline design is vulnerable and leaks data-dependent signature. The TVLA leakage disappears for HP-AES in a DCM mode, which prevents an adversary to improve SNR of the captured signature by turning off other blocks. However, there is a strong need to improve PSCA resistance at IVR input in a CCM mode, which would be discussed in the next chapter.

CHAPTER 6

SECURITY-AWARE IVR DESIGN

The architecture of the IVR presented in the previous chapter represents a generic IVR present in any SoC or high performance processors, i.e. no specific blocks are added to enhance PSCA resistance. Therefore the PSCA protection offered by the previous architecture solely depends on the transformations described in Chapter 3 and Chapter 5. Although various transformations reduce the correlation between the IVR input current and the AES current, the measurement results clearly show that the information leakage through the IVR input current can still be exploited for successful key extraction. One of the possible reasons can be the nature of the aforementioned transformations. Both small and large signal transformations are linear time-invariant (LTI). The absence of time-variance in these transformations causes the data dependent current signatures to spread out to multiple IVR cycles. If the IVRs cycles are properly aligned, the current magnitude of the IVR input will retain the same data-dependency. The asynchronous behavior between the IVR clock and the encryption clock causes the mapping of the load current to IVR input current to be a one-to-many mapping. However, after realigning the IVR input current, a higher number of measurements can recover the data-dependency. In CPA, the MTD of the design can increase significantly due to this effect, as it has been observed in the last chapter. For TVLA, a strong data dependency exists in the load current signature due to the choice of the plaintexts and all three transformations together are not effective to suppress the data-dependency at the IVR input current.

Introducing dynamic time-variance can help in suppressing the data-dependency of the input current. If the IVR edges are randomly delayed, it will be difficult to align the edges to extract information, thus improving PSCA resistance. In this chapter, a simple all-digital loop randomization scheme is introduced that can help to improve PSCA resistance by

randomizing all the three IVR transformations.

6.1 Loop Randomizer

A dynamic time-variance is introduced in the system by delaying the IVR_{CLK} in a pseudo-random fashion. For the proposed architecture, the clock to the DPWM is generated from the sampling clock (2x higher frequency) through a clock divider. The input clock to the clock divider is delayed in a random fashion (Fig 6.1). To achieve this, a delay-trimmer consisting of a series of delay elements, as shown in Fig. 6.1b, has been used. Each delay element consists of two inverters and one multiplexer. The multiplexer can be used to bypass the delay of the inverters and forward the clock directly to the next stage. The prototype test-chip uses 15 such series delay elements. The select of the muxes are driven by a binary-to-thermometer decoder. The decoder is driven by a 4-bit maximal length linear feedback shift register (LFSR). The LFSR structure is shown in Fig. 6.1c. The LFSR output sequence goes through 15 different values generating 15 different delay values. The thermometer output starts from the right as the delay elements in bypass mode bypasses the input clock directly. Fig. 6.1d shows output clock ($COMP_{CLK,RAND}$) waveform assuming a 3-bit LFSR for simplicity. The delay of each trimmer cell is shown as well. $COMP_{CLK,RAND}$ is used to generate the $DPWM_{CLK,RAND}$ through a clock divider. We note that the compensator outputs D_P and D_N are synchronous with respect to $COMP_{CLK}$ and is captured again with respect to $DPWM_{CLK,RAND}$ inside the DPWM engine. The extra delay added by the trimmer cells, even when all the cells are in bypass mode, ensuring that clock path delay is more than data path delay.

6.1.1 IVR Stability with LR

Randomly delaying the IVR switching clock creates steady state perturbations at the output voltage of the IVR. It is important to analyze the loop stability of the IVR when LR is turned on.

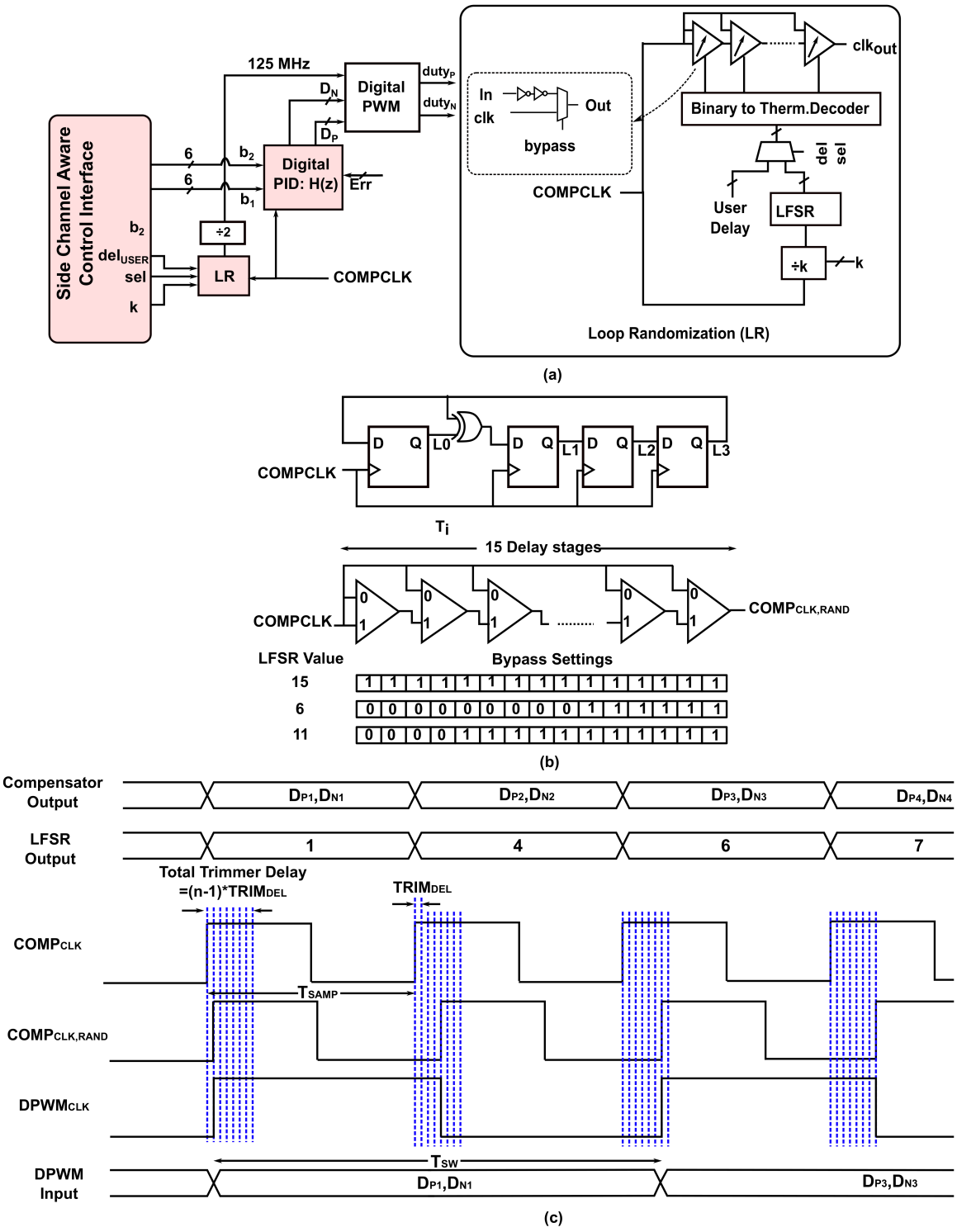

Figure 6.1: (a) Architecture of clock generation scheme for DPWM including clock randomization through LR (b) Circuit diagram of the LFSR and the decoder (c) Timing diagram of different clocks when LR is active

DPWM Architecture

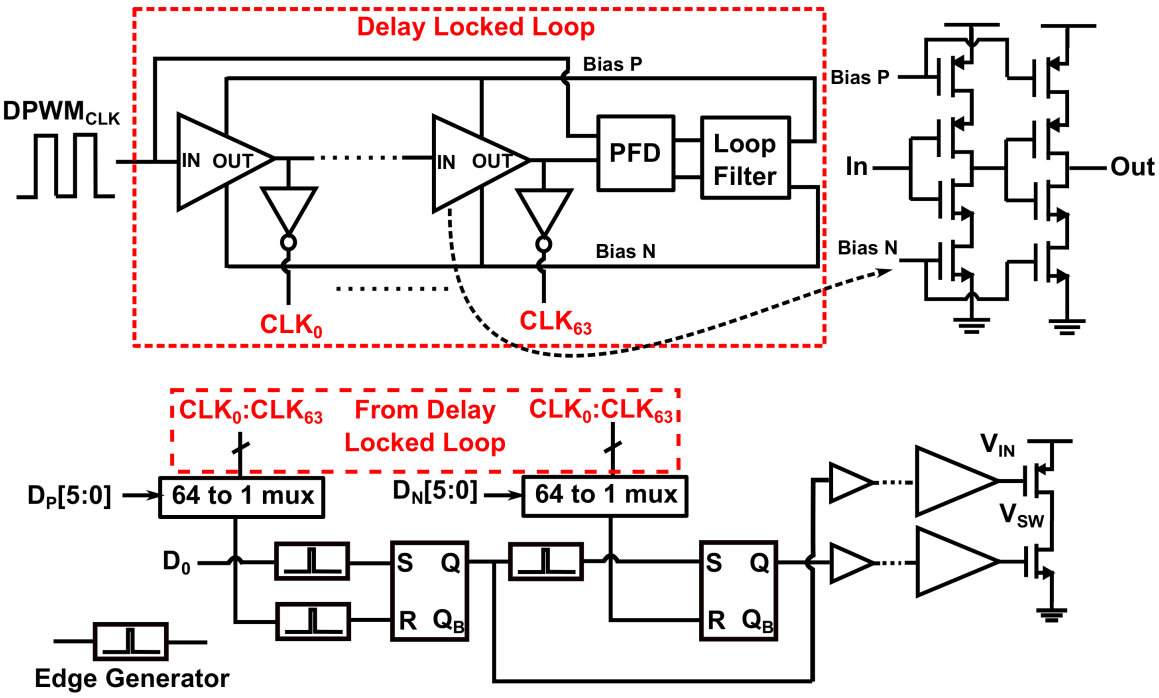

Figure 6.2: Architecture of DPWM

Randomly delaying the input clock to the DPWM can be thought of a higher jitter value at the DPWM clock. In this situation, the architecture of the DPWM plays a critical role in determining the stability of the IVR. The DPWM for the proposed design uses the 2nd sample (latest) in every switching period (two samples are spit out of the digital compensator every switching cycle). The DPWM consists of a delay-locked-loop (DLL) with 64 stages providing a 6-bit resolution. A standard phase frequency detector (PFD) and a loop filter is used to control the delay of the individual cells, as shown in Fig. 6.2.

Stability Analysis

Fig. 6.3 shows the DLL bias voltages, the input and output clock of the DLL and the delay between the input and the output clock edges, when LR is activated. In absence of LR,

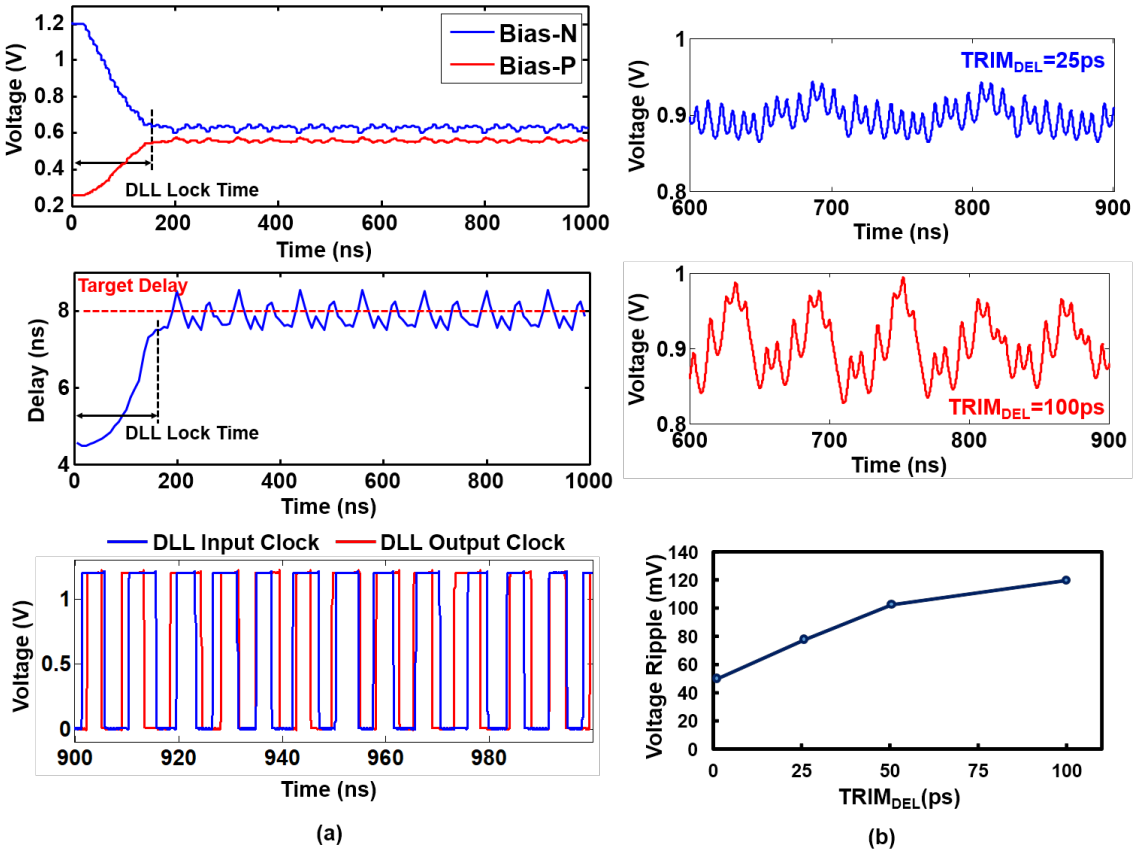

Figure 6.3: (a) Stability of the DPWM DLL with LR active (b) Output Voltage waveforms for different TRIM_{DEL}

the delay between the DLL input and output clock converges to the target delay of 8ns (corresponding to 125MHz IVR_{CLK}). However, when LR is turned on, the bias voltages of the DLL as well as the total delay across the delay chain oscillate around the 8ns target. One can see that the DLL is able to regulate the total delay across the delay chain around the target. The upper and lower limit of the delay can be expressed as

$$\begin{aligned} T_{DLL,min} &= 2 * T_{SAMP} - (n-1) * TRIM_{DEL} \\ T_{DLL,max} &= 2 * T_{SAMP} + (n-1) * TRIM_{DEL} \end{aligned} \tag{6.1}$$

A minimum delay can possibly lead to overlap of the pulse driving M_2 and pulse driving M_1 for the next cycle. To ensure no direct path between V_{IN} and GND, D_N (Fig 5.3) is saturated above a threshold, which ensures that M_2 turns off before the next pulse for M_1 appears. However, when next M_1 pulse appears after $T_{DLL,MAX}$, the inductor current flows through the body diode of M_2 for the longest amount of time, leading to a higher conduction loss. However the power overhead is significantly lower than the situation when the M_1 and M_2 pulses overlap.

The perturbation at the output is directly proportional to delay variation created by the LR. Fig 6.1b shows that as the delay of the trimmer cells are increased, the output ripple increases. For the prototype design, $TRIM_{DEL}$ is kept fixed. However the LR frequency can be adjusted. When LR is driven by $COMP_{CLK}$, the $DPWM_{CLK}$ sees every alternate delay values. As the DLL bandwidth is lower than the $DPWM_{CLK}$ frequency, the DLL is slow to respond to the delay variations as the average delay across the DLL chain remains around the target value. However, if the LR frequency is reduced to 4x or 8x lower, the DLL responds to the delay variation as well as the variations at V_{OUT} are within the control loop bandwidth. Therefore the control loop also starts responding to the output perturbations. This results in lower perturbations at the output node.

6.2 Results

6.2.1 Sample waveforms

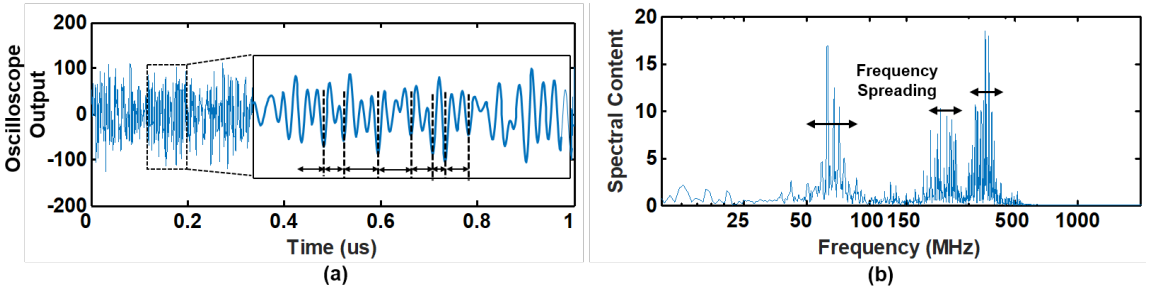

Figure 6.4: $V_{IN,IVR}$ signatures after LR is turned on (a) time domain (b) frequency domain

When LR is turned on, the IVR edges are randomly delayed as shown in Fig. 6.4. The sample captured signature at $V_{IN,IVR}$ are similar for both HP-AES and LP-AES and therefore is shown only once. The FFT of $V_{IN,IVR}$ shows that new frequency components appear in between 50MHz and 100MHz. The frequency spreading originates from the delay sequences in the LFSR as well as the response of the IVR loop to the output perturbations.

Effect of LR frequency: The LR block in the prototype test-chip can be driven at different frequencies, ranging from F_{SAMP} to $F_{SAMP}/8$, F_{SAMP} being the sampling frequency of the controller (ADC and compensator). As already explained in section 6.1, slowing down the LR frequency causes both the DLL loop as well as the IVR control loop to react to the output perturbations. This reduces both the output ripple as well as frequency spreading in the input current. Fig. 6.5a shows the normalized output ripple without the LR and with LR active with different frequencies. As the LR frequency is lowered, the output ripple decreases. Fig. 6.5b-d shows the $V_{IN,IVR}$ spectrum for three different LR frequencies. When LR is running at F_{SAMP}, maximum spreading is observed at the $V_{IN,IVR}$ spectrum as the output perturbation is outside the loop bandwidth. More frequency spreading helps in obfuscating the PSCA signatures, however the output ripple also increases by 3x. For the

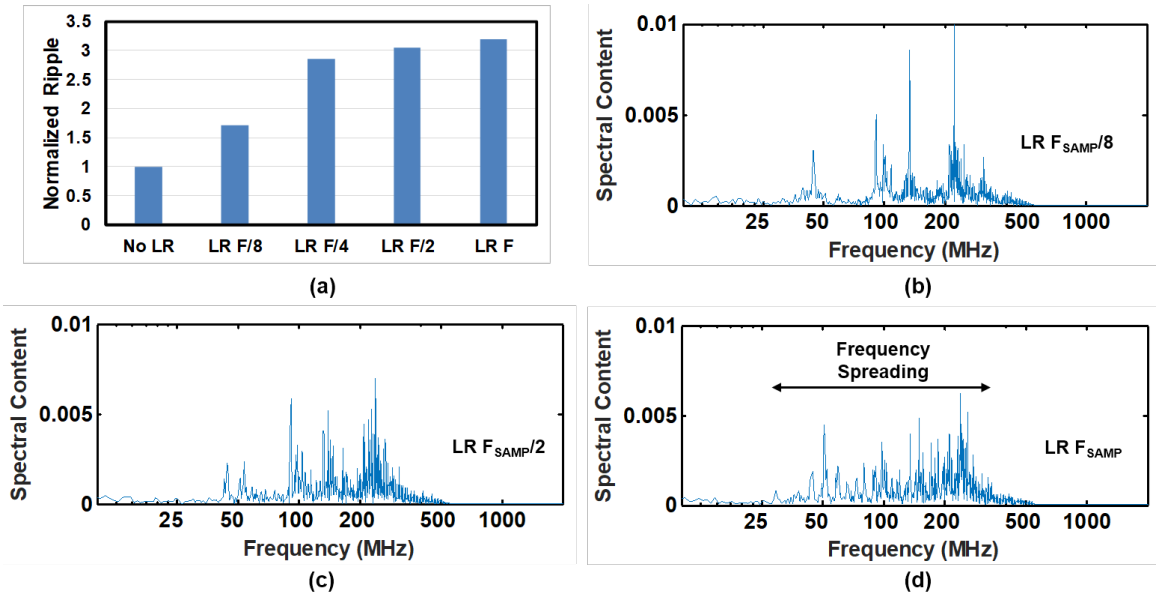

Figure 6.5: Effect of LR frequency on (a) the output ripple and (b-d) the input spectrum

demonstrated results, the LR is driven by $F_{SAMP}/8$.

6.2.2 HP-AES

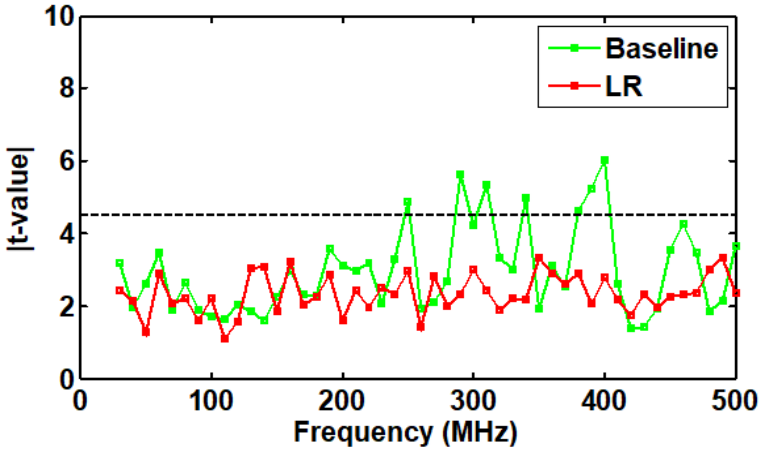

Figure 6.6: TVLA on $V_{IN,IVR}$ with LR on for HP-AES @100,000 traces

TVLA: When LR is turned on, all three transformations through the IVR are randomized. Therefore, aligning the $V_{IN,IVR}$ signatures becomes inaccurate as no constant phase

relationship exists between the captured traces as visible in Fig. 6.4. Fig. 6.6 shows the result of TVLA with LR active, on the HP-AES design. The t-value does not exceed the threshold for all frequency bands with 100,000 traces.

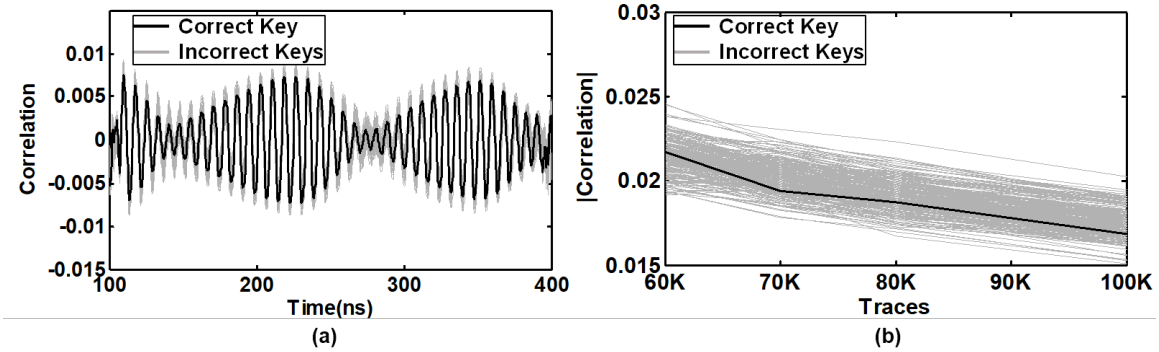

Figure 6.7: CPA on $V_{IN,IVR}$ with LR active for HP-AES (a) correlation against time (b) correlation against traces

CPA: A CPA was also performed on the IVR with the LR turned on. Coherent with the TVLA results, no successful CPA was observed as shown in Fig. 6.7.

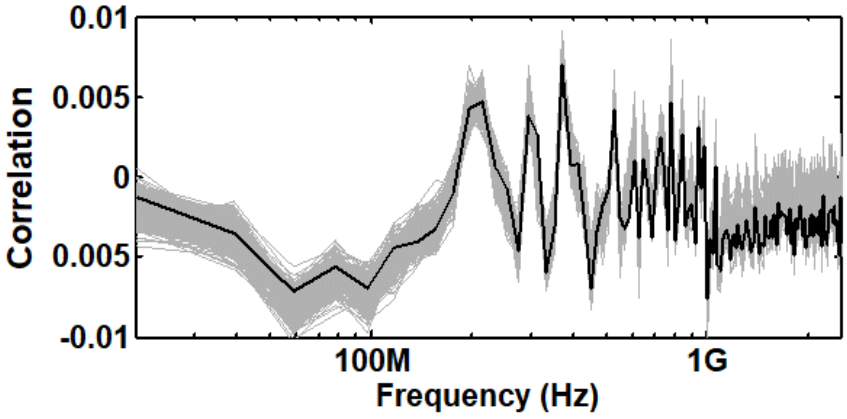

Figure 6.8: Frequency domain CPA on IVR-AES with LR active

Alternate Attacks: It is important to understand whether suppression in leakage in LR mode is contributed only by a time-domain dynamic randomness or a combined effect of randomization of all three transformations. Frequency domain CPA as elaborated in section

5.4.1 is performed with LR activated. Fig.6.8 shows the frequency domain CPA results after turning on the LR. No successful CPA was observed. This result shows that the improvement in PSCA resistance with LR is not solely due to random time-delay in the captured $V_{IN,IVR}$ signatures. The improvement is also attributed to randomization of all transformations of the IVR. Therefore LR is inherently different than existing random-delay based countermeasures. A RTF based attack, as discussed in 3.7.2, was also performed on the $V_{IN,IVR}$ signatures with LR, however no successful TVLA was observed.

6.2.3 LP-AES

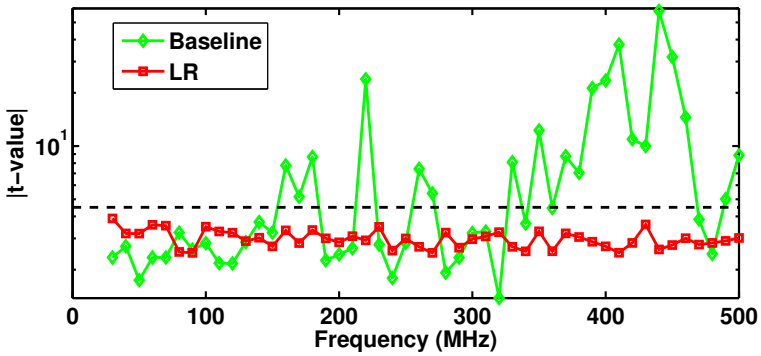

Figure 6.9: TVLA on $V_{IN,IVR}$ with LR on for LP-AES (100,000 traces with alignment without V_{AES})

TVLA: If LR is turned on, no leakage was observed on $V_{IN,IVR}$ across all frequency bands of filtering. The baseline IVR, shown in Fig. 5.21 was extremely vulnerable to TVLA, with $\leq$ 1000 traces required to exceed the 4.5 threshold. Coherent with the HP-AES results, this clearly shows that LR can successfully block leakage at the IVR input.

CPA: For the LP-AES architecture, when LR is activated, no successful CPA was observed on the IVR input with 100,000 measurements. Fig. 6.10 shows peak correlation against traces and frequency for all possible key guesses. LR improves the MTD of the design by 100 times, compared to a MTD of 1000 of the standalone design, shown in Fig. 5.22.

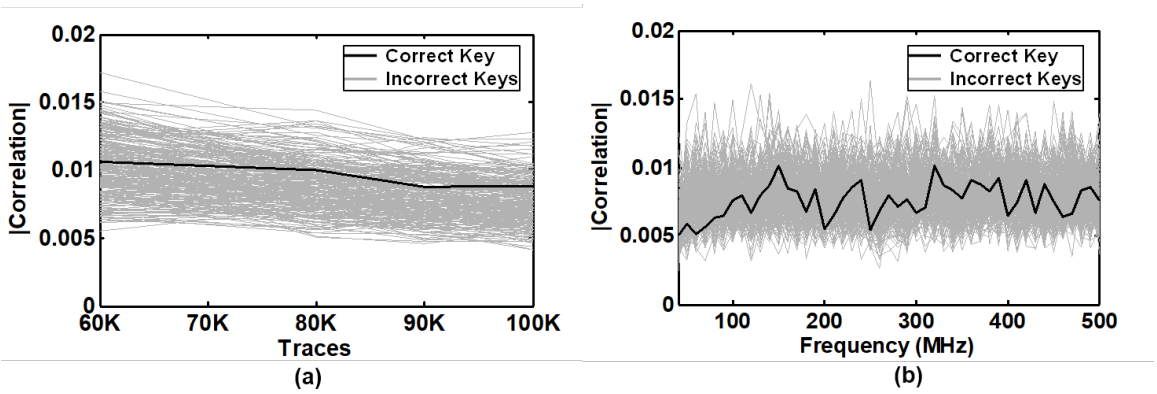

Figure 6.10: CPA on $V_{IN,IVR}$ with LR on for LP-AES (a) correlation vs. traces (b) correlation vs. filter frequency

6.3 Performance Impact

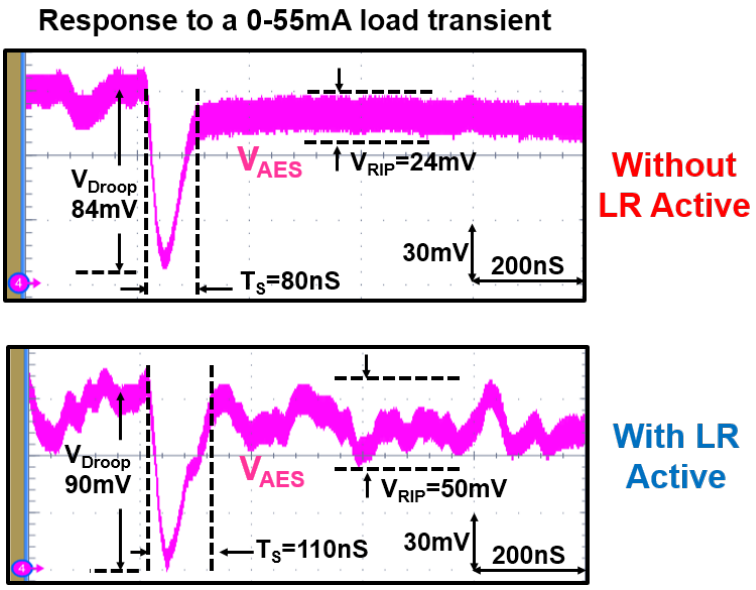

Figure 6.11: Steady state ripple and transient performance without and with LR active

6.3.1 F_{MAX} of Encryption Engine

Turning on LR causes the steady state output ripple to increase and might cause the underlying logic to incur a timing violation. The increased output ripple, shown in Fig. 6.11, reduces the maximum achievable frequency (F_{MAX}) the encryption engine can run at. Fig. 6.11 also shows the response of V_{OUT} to a sharp load transient before and after activating LR. LR increases the voltage droop by 6mV and settling time by 30ns.

To characterize the reduction in F_{MAX}, a large number of AES encryptions are performed before and after turning on LR and the maximum frequency at which all encryptions were executed without functionality failure is found out. Turning on LR causes 3% degradation in F_{MAX} of the AES engine.

6.3.2 System Power Overhead

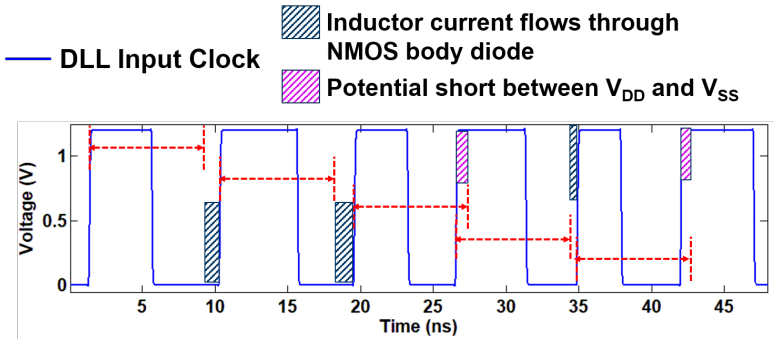

Figure 6.12: Sources of power loss in LR mode

As discussed in section 6.1.1, D_N is saturated above a threshold to ensure no overlap of gate signals of M_2 and M_1 for the next cycle. This leads to a portion of every clock cycle when none of the transistors remain on. The LR is typically tested with the IVR is CCM mode and therefore the remaining inductor current, after M_2 turns off, flows through the body diode of M_2. This increases the conduction loss and leads to 5% increase in total power consumption (IVRs input power) when the IVR is driving a parallel load of 60mA, along with the AES at a 0.85V output voltage.

6.3.3 Performance Comparison

Table 6.1 compares the proposed security aware IVR design and its overheads with selected ASIC based generic/logic-style based countermeasures. The low overheads of the security aware IVR design and ease of integration into an existing IVR design make the proposed techniques attractive for implementation.

6.4 Summary

Randomizing the IVR control loop by randomly delaying the gate signals of the power stage transistors is shown to reduce the information leakage at the IVRs input. The improvement in PSCA protection is not only attributed to the enhanced misalignment effect, but also the randomization of small-signal and large-signal transformations as well. Results for both HP-AES and LP-AES show no signs of leakage in TVLA as well as no successful CPA attack with 100,000 measurements, yielding a 20x and a 100x improvement in MTD for HP-AES and LP-AES respectively. The proposed circuit is all-digital, can be synthesized and easily integrable into existing architecture for inductive IVRs. The 3% performance overhead and 5% power overhead can easily be traded off with no requirement of algorithm/architecture/physical-design modification in the existing AES design. Although inductive IVRs, in their default architecture (baseline) and with the proposed loop randomization scheme, are shown to be effective for improving PSCA resistance, it is important to analyze the role of inductive IVRs in EM side channel resistance, another commonly used side channel. This will be elaborated in the next chapter.

Table 6.1: Performance comparison against selected existing countermeasures

Parameter	This Work [64]	VLSI15 [70]	ISSCC09 [30]	ISSCC11 [82]
Technology	130nm	65nm	130nm	130nm
Standalone AES Power/Freq.	10.5mW/40MHz	98.0mW/1.32GHz	33.32mW/100MHz	-/50MHz
Operating Voltage (V)	0.45-1.05 (from IVR)	0.41 (External)	1.2 (External)	1.2 (External)
Power Overhead	Power	5%*	-30%	33%
Area Overhead	2135 μm^2 (103 gates) $	0.194mm2 (2x)	0.079mm2 (20%)	11000 gates (67%)
Performance Overhead	3.33%&	0%	50%	0%
Countermeasure Type	Integrated Voltage Regulator	Charge-Recovery Logic	Switched-Capacitor Current Equalizer	Duplicated Data Paths
Analysis Method	CPA, TVLA	DPA	DPA	CPA/Fault Attack

*Total increase in IVR+AES system power after turning on the LR with 60mA parallel load along with AES, $ Area of the synthesized LR block, & Performance overhead calculated from Fmax impact due to higher droop (increase in supply guardband) with LR on

CHAPTER 7

ELECTROMAGNETIC SIDE CHANNEL CHARACTERIZATION

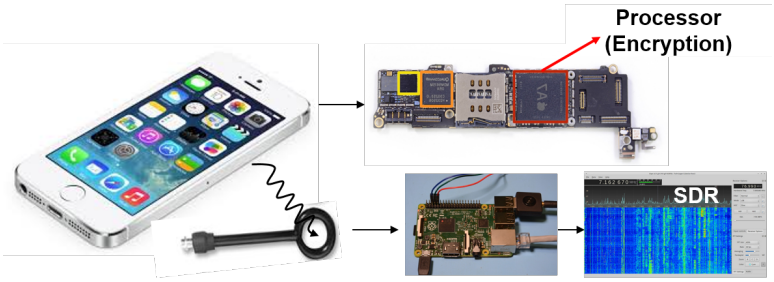

Figure 7.1: A EM attack on a practical gadget

Performing a successful power attack in a practical environment requires the adversary to physically probe the target device. The physical probing, although feasible in a lab environment, requires direct access to the printed circuit board (PCB) or the SoC package or the charger/power supply socket for electronic gadgets. Even if the supply line leaks compromising signatures, a power attack might be infeasible due to the following reasons as shown in [99].

1. It might be difficult to tap the supply line on the PCB as supplies of ICs are often routed using the unexposed inner layers of a multi-layer PCB.

2. A digital processor or a SoC typically comes with multiple supply lines dedicated for different purpose. For example, in a FPGA, three on-board LDOs supply power to digital, I/O and analog portions. Moreover a large chip typically has multiple parallel power pins to reduce the worst case IR drop across the PDN. Therefore, it might be difficult to identify which power pin to tap for signature measurement.

3. Power attack requires measuring the current signature of the underlying platform and typically a series resistance is inserted in the power path to measure the supply cur-

rent as a voltage drop across the resistance. However, performing this for a practical scenario requires a PCB with space between the output of the external VRM and the input pin of the chip, which might not always be present, particularly for a densely packed PCB. One can rely on single ended measurement where the voltage fluctuation directly at the supply pin of the chip is measured. However the magnitude of voltage fluctuation is dependent on the effective resistance of the PCB trace looking from the chip to the external power supply.

4. Moreover state-of-the-art gadgets may come with an in-built sensor that can detect whether the supply line is being probed by sensing the change in capacitance in that node.

A commonly used side channel is electromagnetic emanations from the target platform [9, 100]. The electromagnetic emanations generate from the magnetic fields created due to change in current through a wire which includes the lower level interconnects in a chip, top level metal routing as well as bondwires or package connections. Power and EM side channel are related to each other as both side channels are function of switching currents of the logic gates which are data dependent. A major difference between the power and the EM side-channel measurement is capturing EM side channel is completely non-invasive and can be performed with inexpensive EM probes [65] (Figure 7.1).

Although the source of EM leakage is the fluctuation of the power dissipation, a countermeasure that inhibit power attack is not guaranteed to inhibit EM attacks. Countermeasures for PSCA prevention can broadly be classified into hiding and masking based techniques. Masking based countermeasures like [29] modify the computation at the intermediate steps of the algorithm and can potentially prevent EM leakage. A logic style or architecture based countermeasure like the use of duplicated AES datapath as proposed in [82] improves resistance of both power and EM side channels. However, generic countermeasures which typically *hides* the power signatures might not be effective for hiding the EM signature. This is solely due to the fact that EM emissions from the encryption

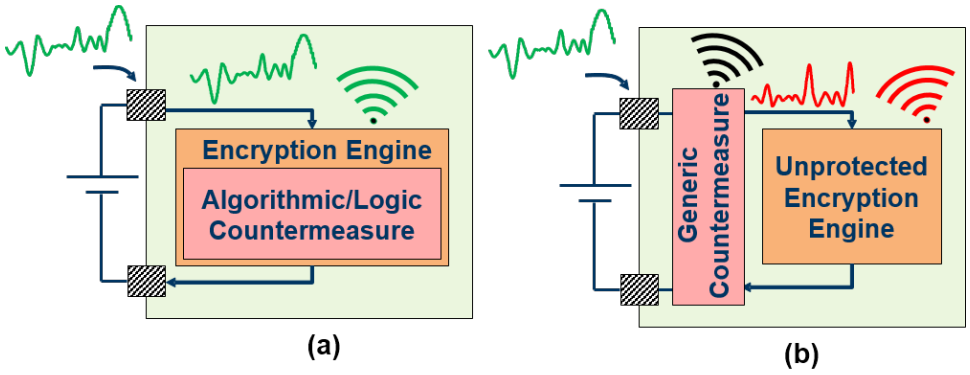

Figure 7.2: Effect on EM leakage for different classes of countermeasures for power attack (a) Algorithmic/logic style based (b) Generic Countermeasures

engine is not modified and can be captured if a suitable probe is used near the encryption engine. For example, a number of generic countermeasures isolate the supply and ground nodes of the encryption engine from the external power pins [15, 74, 30, 84] (Fig. 7.2), however, their effectiveness against EM leakage is not demonstrated. A hiding based generic countermeasure which can prevent against both power and EM leakage can save significant power, performance, area and design-effort overheads associated with the traditional algorithmic and logic-style based countermeasures, both for high-performance and resource-constrained systems.

7.1 Motivation

The inductance in an inductive IVR carries continuously switching current which creates a strong EM radiation source from the inductance. Moreover, as the input current flowing through the power stage has sharp transitions, a strong EM signature is also generated from the parasitics of the package elements to the IVR input. Figure 7.3 explains the EM signatures measured near an inductive IVR which drives an encryption engine. The EM signal measured by an adversary is the result of the interference of the EM signature from the encryption engine as well as the same from the integrated inductance and other parasitics. However, as the inductor current and IVRs input current are complex transformation of the

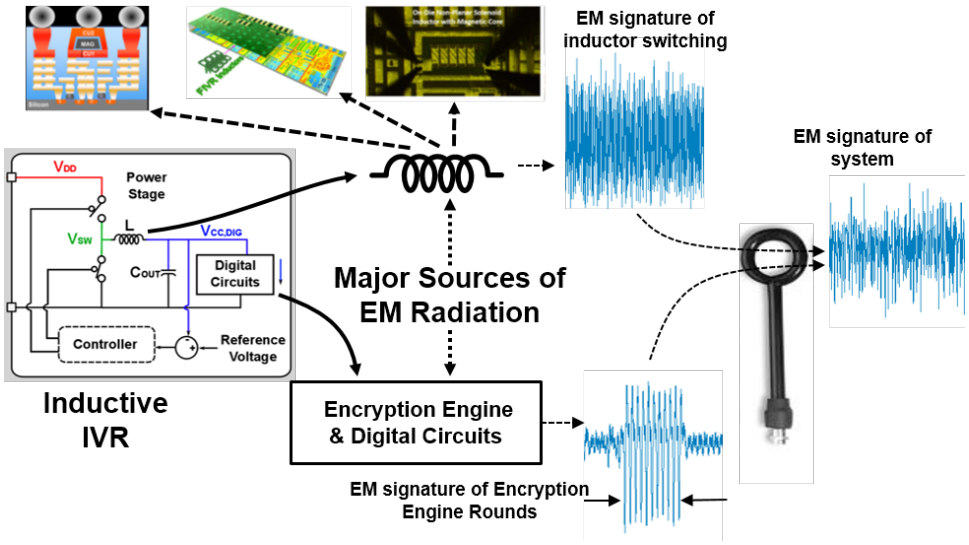

Figure 7.3: Explanation of EM signatures measured from an inductive IVR

AES current, the measured EM signal can potentially weaken the correlation between the measured signature and the switching activity of the AES. As passives in inductive IVRs are integrated within a small volume, spatially separating the EM emanations from these two sources might be challenging, particularly in a practical attack scenario where the adversary does not have access to a fine probe ($\leq$1mm resolution) with the targeted hardware affixed to a mount table. The separation of these signals will be even more challenging if the inductance is integrated in form of on-die [55] or thin-film inductance [60]. Introducing additional randomness within the IVRs control loop can further reduce the correlation. Therefore characterizing the EM side-channel signatures from an inductive IVR driving an encryption engine is important.

7.2 Prototype System

The test-chip presented in chapter 5 is used to characterize the EMSCA resistance of a system of an inductive IVR driving an AES engine. The PCB used for measuring power signatures is simplified with the removal of the series resistances and the amplifier for power signature measurements. The new PCB is shown in Fig. 7.4.

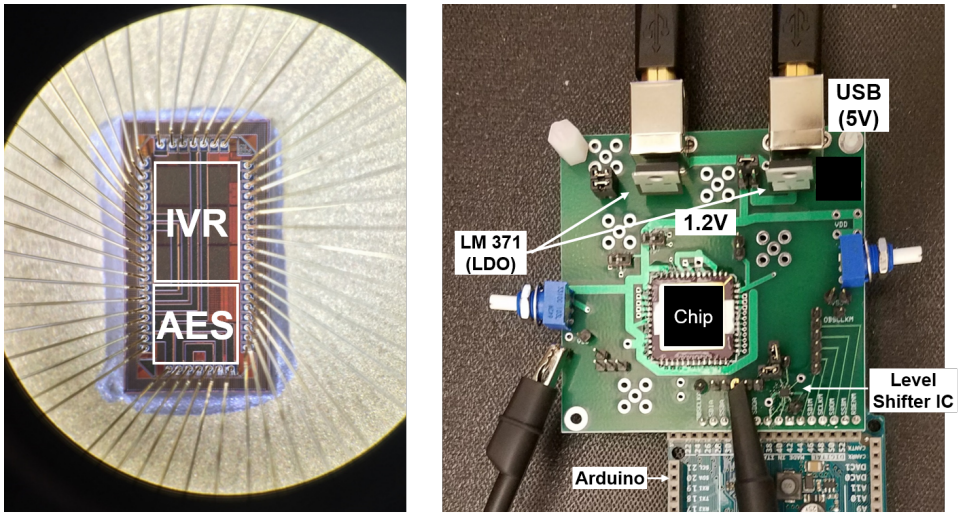

Figure 7.4: (a) ASIC Micrograph with bondwires (b) Prototype PCB for characterization

7.2.1 System Design

The chip is powered by standard USB connections. An off chip voltage regulator (LM317) is used to convert 5.0V from the USB to 1.2V supply for the IVR input. The off-chip LDO also represents a typical power supply architecture when an IVR isn't present in the system. The plain-texts and key of AES encryptions are communicated to the chip in the same fashion described in Chapter 5.

7.2.2 Chip Packaging

For commercial systems, every silicon die would be accompanied with a package which forms the connection with the PCB. Packages play a critical role in leakage of EM side channel signature as different components of the package, mostly the parasitic inductance can amplify or mask the desired signatures. The ASIC is packaged in a Leadless Ceramic Package (LCC). Figure 7.4 show the structure of a LCC package. The pads on the die are attached to the package with bondwires.

Compared to lower parasitic inductance and resistance of a C4 or a QFN packages, the higher parasitic inductance of the bondwires in a LCC package can amplify the EM

emission, and hence, preventing EM side channel leakage from such a package is more challenging.

7.2.3 Classification of EM Signatures

The EM emissions from the system of the IVR and AES, like any other systems, can be classified into two classes [80]. The conductive EM radiations are due to the current variation in different interconnects of the chip. Measuring a conductive EM emission requires a probe with fine spatial resolution with proximity to the actual current carrying interconnect. For an IVR supplying AES, the bondwires carry the IVR supply current to and from the chip. Due to proximity to the current carrying conductor, conductive EM signatures should have similar properties as the power signature on that corresponding line. Measuring conductive EM emission for extracting key from an AES engine requires accurate placement of the probe and is dependent on a multitude of other factors like the physical design of the AES engine and the clock and the power grid routing. Moreover, measuring conductive EM signatures is extremely sensitive to noise from other interconnects in close proximity.

The second major source of EM emission is coupling between the desired signature and a strong carrier like the clock. Such a carrier signal can be demodulated to recover the original signature. Due to the integration of the VR in the same die as the AES, the couplings between the encryption core and the passives of the IVR will be significantly higher. This coupling effect is enhanced when the IVR supplies the AES as the IVR switching frequency component at the AES supply modulates the EM radiation from the AES.

One possible option of hiding the EM signature from the encryption engine is to place a strong EM radiator close to the encryption engine. An inductive IVR achieves exactly the same effect without adding any extra elements. However, it will be shown in section 7.4 that, a strong EM radiation near the AES engine will simply be equivalent to an additive noise in the measured EM traces. It will reduce the SNR of the measured signatures and partially increase the side channel resistance of the AES, however, does not

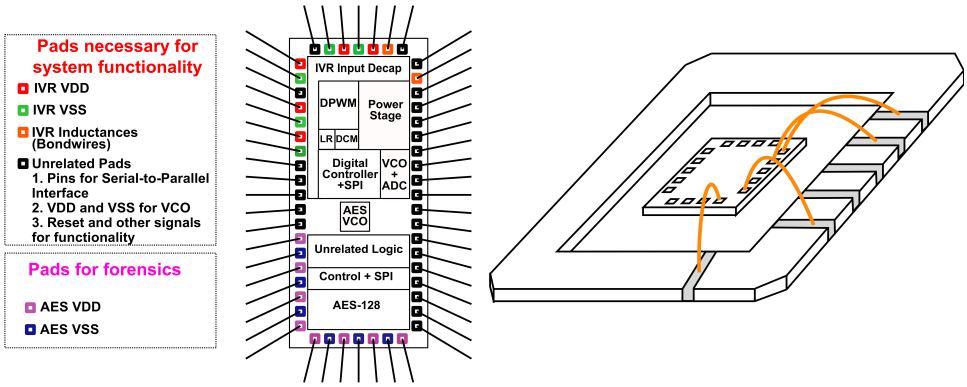

Figure 7.5: Silicon die and the corresponding LCC package with pads details

eliminate/reduce the information leakage in the captured EM signatures. Moreover, if the frequency of the EM radiation is different than the frequency of interest, simply filtering or demodulation can be effective to remove the noise effect. The effect of EM emission from the inductor when the AES is powered by IVR is different from simply keeping a strong EM radiator near the AES engine. Therefore, the interaction of the AES and the IVR is a key factor in improving resistance to EM SCA attack.

7.3 Measurement Methodology

7.3.1 Measurement Points for Forensics

Figure 7.5 shows the different pads of the ASIC and their corresponding pins in the package that carry side channel signatures. A set of pins and probing points are dedicated for forensics of the designed ASIC. These pins will not be present in a practical SoC or microprocessor, however, probed out of the test-chip to be able to power the AES engine directly from the off-chip LDO. The power ($V_{DD,AES}$) and ground ($V_{SS,AES}$) of the AES are probed out for this purpose. The pins which do not carry side channel signatures are marked in black.

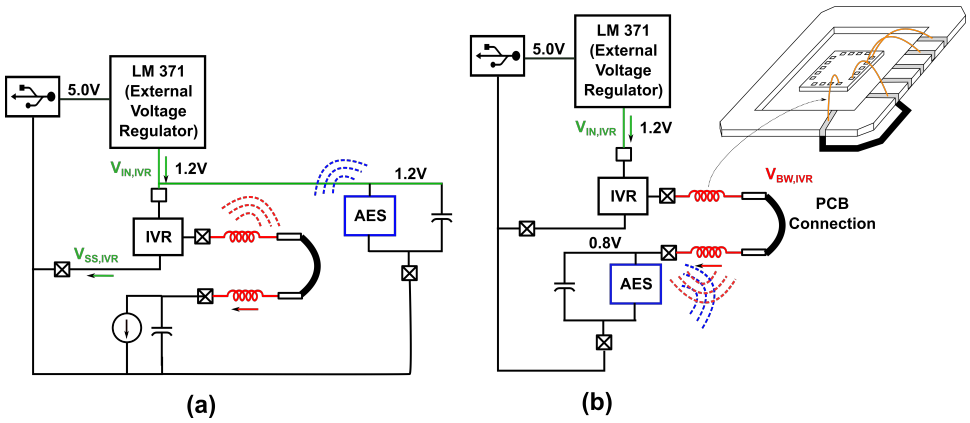

Figure 7.6: Measurement scenarios a) AES is powered by an external voltage-regulator and b) IVR is powering AES engine

7.3.2 Measurement Cases

Two measurement scenarios are considered as depicted in Figure 7.6. First, the AES engine is powered using the off-chip voltage regulator (LM317), which represents a traditional off-chip power delivery system. To prove the point that having a strong EM radiator near the encryption engine will have an insignificant effect on the EM leakage, the IVR is kept on i.e. the IVR drives a steady load current and the transistors M_1 and M_2 switch continuously. Naturally the inductor carries switching current and radiates strong EM signatures. However, as the IVR does not supply the AES engine, the inductor current and the corresponding EM emission have no relation to the AES current. In the next setup, the AES engine is powered using the IVR's output. Two different control loop settings of the IVR are used

- A baseline configuration where no randomization is activated, resembling the behavior of a generic IVR
- Randomization in the control loop of the IVR activated as proposed in [64]

For the following experiments, HP-AES is used as the chosen AES architecture.

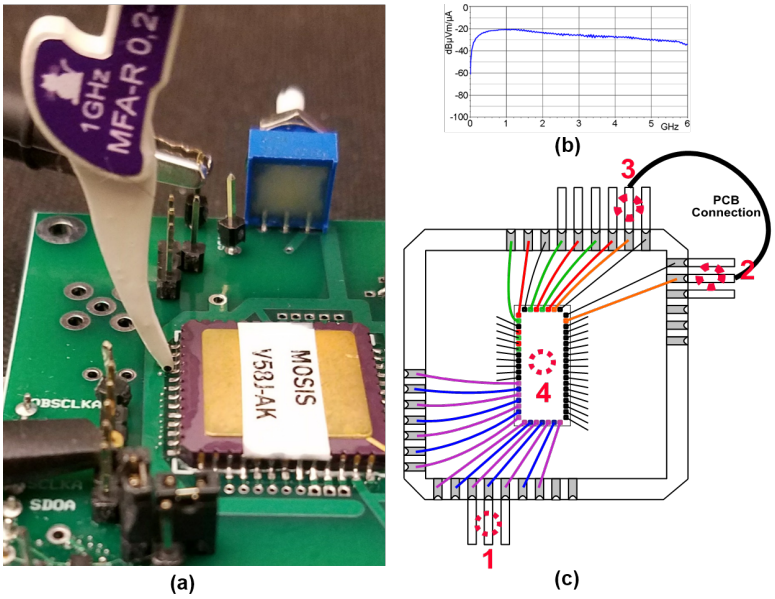

Figure 7.7: (a) Forensic probe used for characterizing the EM emissions from different parts of the ASIC (b) Probe characteristics: received power vs frequency (c) Probing locations on the package pins

7.3.3 EM Probes

The key component of any EM signature measurement is the choice of the EM probes. EM probes used for capturing side channel signatures can be classified into near field probes and far-field probes. Far-field probes are used for capturing low-frequency signatures ($\leq$1MHz) over a longer period of time. For a far-field probe, measuring either the electric field or the magnetic field is enough. For near field probes, the electric and the magnetic field are related in a complex manner. Near field probes can measure either the magnetic field or the electric field. Magnetic field which is generated from the current fluctuations in a conductor is effective in revealing side channel signatures. The quality of the measurement is determined by the diameter of the loop antenna (which also relates to capture bandwidth). A smaller loop diameter provides higher spatial resolution, however the measured signatures can be weaker due to smaller loop area. A large loop generates higher magnitude of magnetic field, however spatial resolution is limited as well as the bandwidth of the mea-

surement. A large loop can actually limit the magnitude of the measured signature if the distance from the signature generating spot is higher due to inability of moving the probe.

A commercial fine resolution active probe is first used for characterization of the EM leakage from different pins of the IVR as shown in Figure 7.7. The EM probe (Langer) measures magnetic field with a 300μm resolution. An active low noise amplifier is used to pick up EM signatures from individual pins of the package. Moreover, the high bandwidth (6GHz) of the probe allows accurate measurement of the high frequency EM radiations from the package bondwires. However, due to extremely small loop diameter, the amplitude of the measured signature is extremely sensitive to the distance of the probe and the package pin. Therefore, physical access to the individual pins is necessary to use these kinds of commercial EM probes as demonstrated by [65]. Therefore this scenario matches more closely to a testing environment rather than a real attack on a PC or a device executing encryption. This probe is referred as *forensic probe*.

Figure 7.8 shows two EM probes (Beehive Corp.), which are commonly used for EM attack on PCs and smartcards [101]. Most importantly, these probes can capture signature at a distance from the target chip. The corresponding frequency response of the power of the captured signatures is also shown. The large loop antenna is suitable where the system limits the physical distance between the silicon die and antenna place as used in [80]. The diameter of the large loop antenna is comparable to the size of the package. Therefore, the probe is always placed in location 1 annotated in the figure. The EM probe with a smaller loop antenna (referred as small loop attack probe) is also suitable for places where the system prohibits physical proximity to the pins of the IC. Due to the smaller diameter of the loop, the measured signature differs based on the location of the probe with respect to the package. Due to the smaller loop diameter, the measured signatures are attenuated compared to the large loop probe, however a higher bandwidth allows this probe to pick up high frequency signatures.

As mentioned in prior works, low-cost EM side-channel attacks are mainly performed

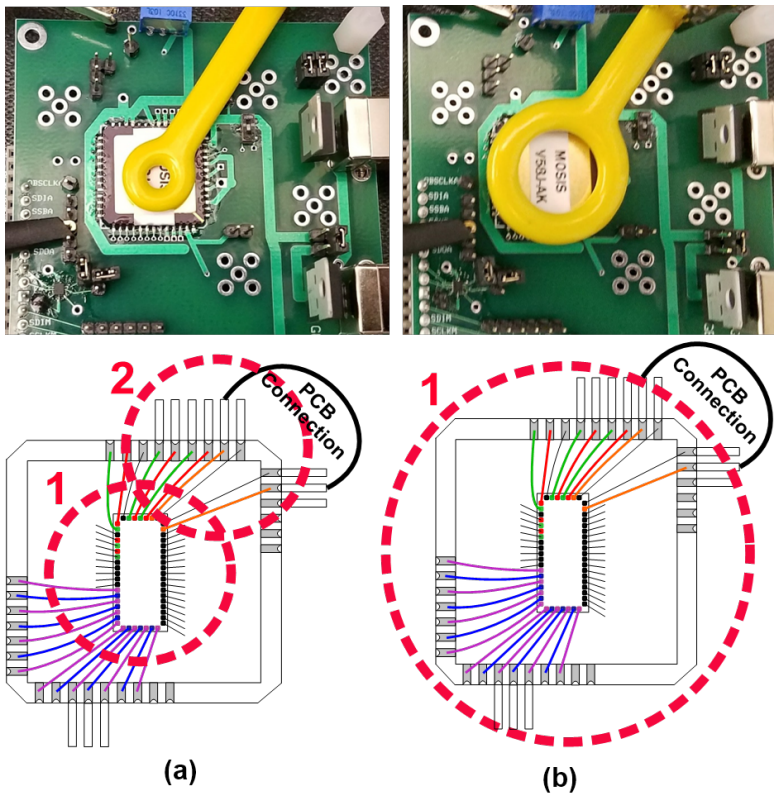

Figure 7.8: Attack probes used to resemble practical attacks on the ASIC (a) Small loop attack probe (b) Large loop attack probe

using loop antennas, the large loop and the small loop attack probe. Therefore, the EM side-channel leakage in the prototype system will be quantified mainly using these probes. The probing locations of these two probes are shown in Figure 7.8. The result from the forensic probe will be mostly used to provide better insight into the EM leakage from different parts of the chip and generate measurement based intuition behind the experimental data obtained for more practical low-cost attacks.

7.3.4 EM Characterization with Forensic Probe

AES engine supplied by the off-chip LDO: When the AES engine is supplied by the off-chip LDO, the forensic probe is placed in location 1, near the supply ($V_{DD,AES}$) and ground ($V_{SS,AES}$) line. The supply and the ground current of the AES flows through the

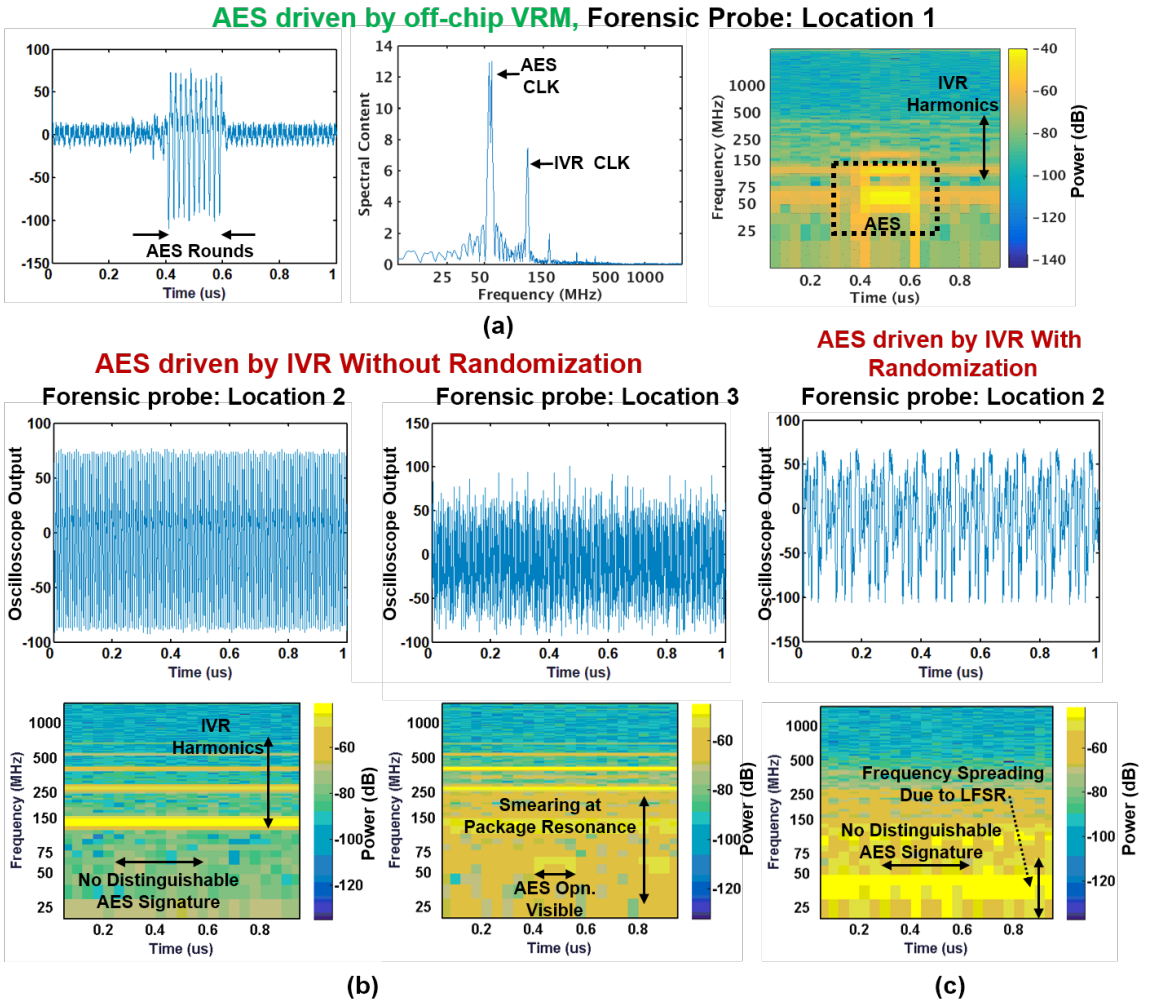

Figure 7.9: Sample EM signatures captured using forensic probe for an AES encryption when (a) AES is powered with the external VRM, (b) AES powered with IVR without and (c) with control loop randomization

bondwires marked in pink and blue respectively. The IVR remains on, however, does not supply the AES. The signatures picked up by the probe in this condition is shown in the Figure 7.9a. The left figure shows the time domain waveform of the measured signature for one entire AES encryption, the middle figure shows the corresponding FFT and the bottom figure shows the spectrogram. The forensic probe due to its proximity to the package pin picks up clean signatures of the 10 rounds of the AES. The interference at the IVR clock

is also picked up however is significantly lesser in magnitude as the IVR clock does not interact with the AES clock, rather is present as an additive EM interference. From the spectrogram, the duration of the AES encryption can clearly be figured out.

AES engine supplied by the IVR: When the AES engine is supplied by the IVR, three locations in the ASIC can potentially emit compromising EM radiation: the AES ground ($V_{SS,AES}$), the IVR input ($V_{IN,IVR}$) and the PCB connection between the two bondwires, referred as V_{BW}. $V_{SS,AES}$ is purely a forensic node as AES current would flow through the common ground ($V_{SS,AES}$) in a practical system. V_{BW} is connected to $V_{DD,AES}$, through a bondwire and is a potential source of radiation.

The signatures picked up by the forensic probe at these locations and their corresponding spectrogram is shown in Figure 7.9b. The signature picked near $V_{SS,AES}$ is similar to AES signature as shown in Fig. 7.9a. This has two important insights: 1) if a finer resolution die-probe is placed closer to the AES, it can pick up the side channel signatures and 2) the AES ground should be internally shorted to the common ground of the chip. The spectrogram of the signatures at V_{BW} (Figure 7.9b) shows the harmonics of the IVR clock, however no distinguishable AES region can be identified. The spectrogram of the EM signatures at the $V_{DD,IVR}$ node is smeared with multiple components at frequencies between the AES clock and the IVR clock. This is due to the fact that the current flowing through $V_{DD,IVR}$ switches between high current (when M_1 is on) and near zero current (when M_1 is off, M_2 is on). This causes the voltage node to ring at the resonance frequencies dictated by the parasitics of the package.

The signature picked up by the forensic probe is EM emission due to conduction as the probe is placed right on top of the pin carrying current. The forensic probe picks up poor signature when placed at location 4 as these probes are suitable only for pickups from package pins. Therefore the behavior of the captured signatures using a forensic probe would be similar to a behavior of the corresponding nodes in power SCA.

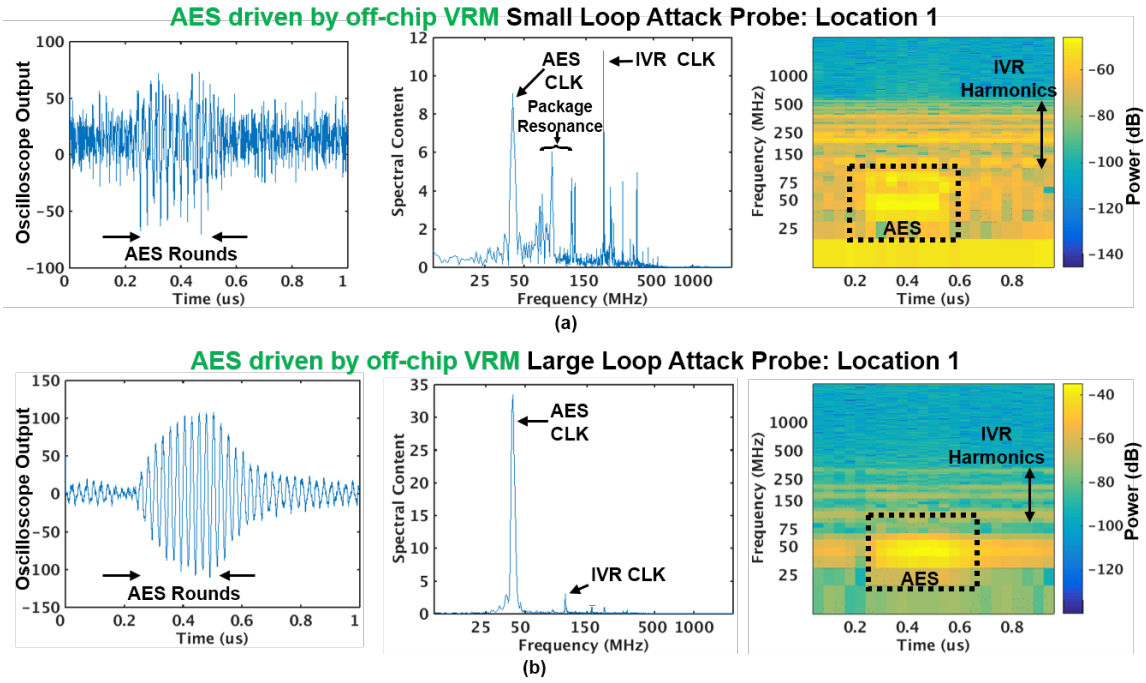

Figure 7.10: Sample EM signatures for an AES encryption when AES is powered with the external VRM using (a) the small loop attack probe and (b) the large loop attack probe

7.4 Experimental Results

7.4.1 Characterizing Attack Probes

The two attack probes were used to pick up signatures corresponding to the two measurement scenarios described earlier. Figure 7.10 shows the sample measurements for both the loops when the AES engine is driven by the external VRM. For the small loop attack probe, EM radiations at a wide range of frequencies are picked up due to high loop bandwidth, however the peak-to-peak amplitude was 4mV (Figure 7.10). The oscilloscope voltage steps were 1mV/division, therefore only 4-bit dynamic range was obtained for the output data. The spectral magnitude of the AES clock frequency is lower than the spectral magnitude at other frequency components, which includes IVR clock as well as package resonance frequency. The spectrogram is smeared with components at the package reso-

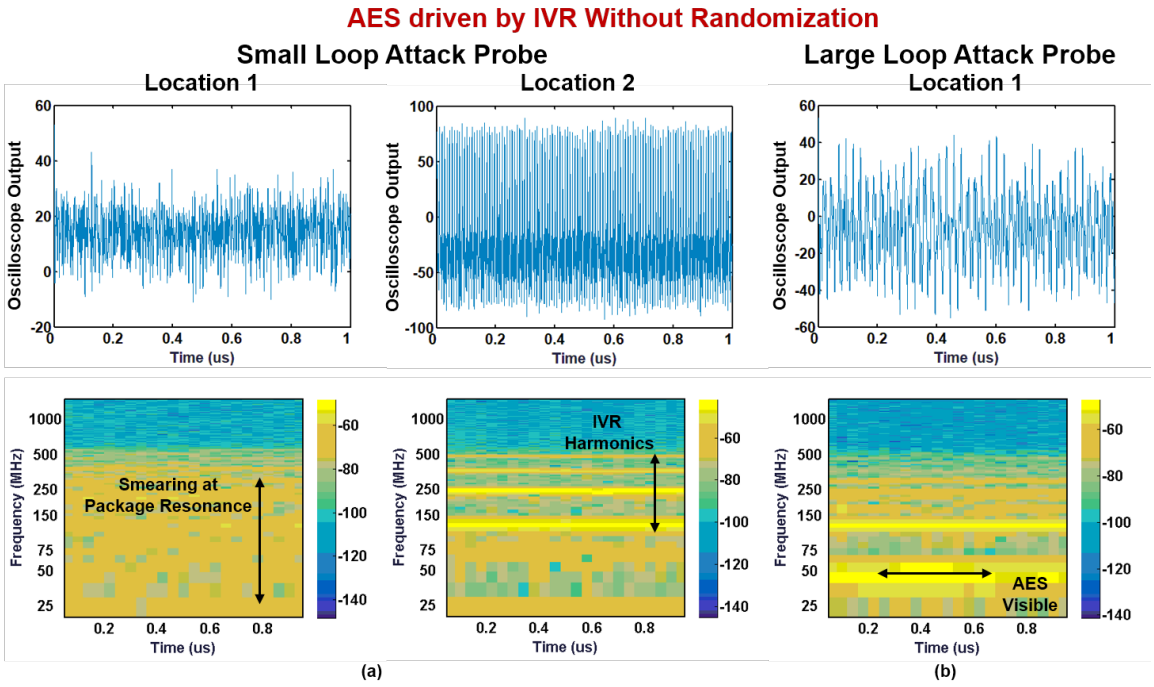

Figure 7.11: Sample EM signatures with the attack probes for an AES encryption when the AES is powered with the IVR using (a) the small loop attack probe and (b) the large loop attack probe

nance frequencies. For large loop attack probe, the spectral magnitude of the AES clock is the maximum which results in a clean AES signature both in the time domain and spectrogram. The higher frequency components are attenuated by the limited bandwidth of the probe (100MHz). The dynamic range of the signature is 80mV peak-to-peak covering the full 8bit resolution of the oscilloscope. Although the IVR continues to switch during these measurements, the AES can clearly be identified from the spectrogram.

The signature picked up by the attack probes when the AES engine is supplied by the IVR are shown in Figure 7.11. Interestingly, for both locations in the small loop attack probe, no visible signature of the AES event can be identified in the spectrogram and both locations observe components at package resonance. As the probe is moved from location 1 to location 2, components at the IVR clock frequency and its harmonics increase due to

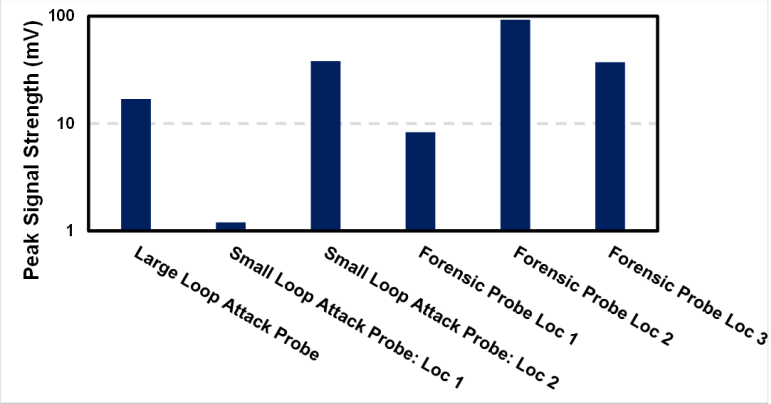

Figure 7.12: Peak-to-peak amplitude of the EM signals for different probes at their corresponding locations

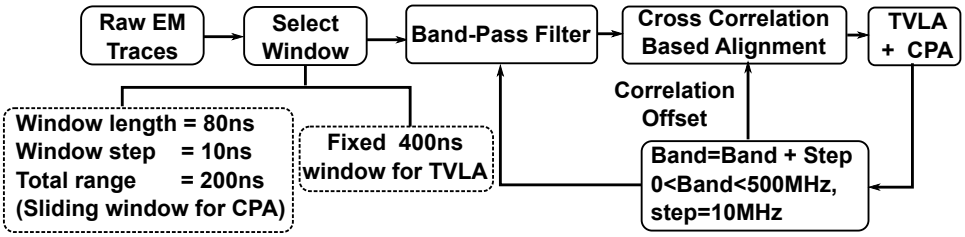

Figure 7.13: Post-processing of the traces for alignment

proximity to the package pins. For the large loop, the AES event is visible in the spectrogram, as the probe bandwidth attenuates the IVR clock, and its harmonics significantly, increasing SNR of the measurement. Figure 7.12 shows the peak-to-peak magnitude of the recorded signals for different probes. The magnitude of the conduction EM signatures picked up by the forensic probe at V_{BW} is highest. The peak-to-peak amplitude reduces for attack probes due to their distance from the emanating sources. Although the amplitude of the large-signal-probe is typically higher due to a larger loop area, the offending component at IVR's switching frequency is outside the probe bandwidth.

7.4.2 Signal Postprocessing

Aligning the captured traces based on the rounds or steps of the encryption engine is critical for leakage analysis of the captured traces. However, as we explained in section III,

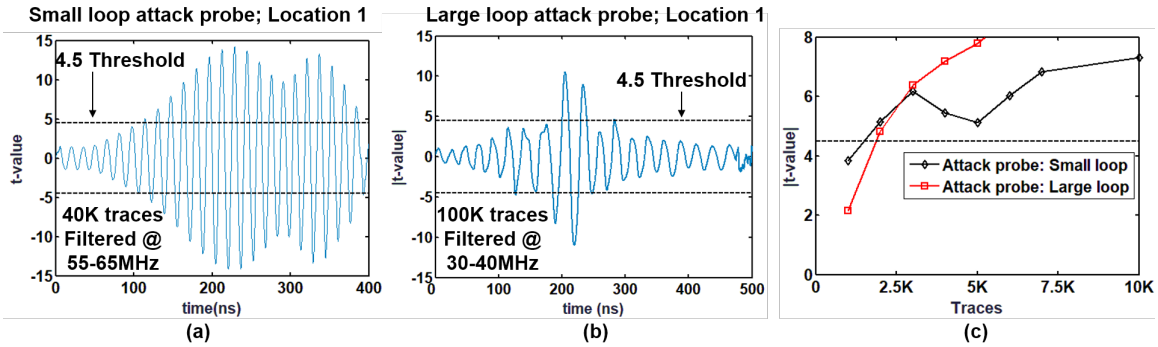

Figure 7.14: TVLA (100K traces) with AES powered with the external LDO with (a) the small loop and (b) the large loop probe (c) Peak t-value against traces used

mapping of the AES rounds to the IVR phases are randomized. For coupled EM emission, demodulation of the carrier signals have been used [80]. We use bandpass filters for processing the captured traces. Filter bands from 10MHz up to 500MHz is covered with a passband width of 20MHz. This replicates the action of a tunable receiver or a demodulator often used in a low-cost EM attack [80]. The filtered signals are aligned using cross correlation with the offset limit bounded by the filtering frequency. The post processing flow is shown in Figure 7.13.

7.4.3 TVLA Results

A *semi-fixed dataset* is used for all TVLA results [98], i.e., each entry in the second dataset (section 5.3.2) are unique, but satisfies the criteria described in [98]. To generate the semi-fixed dataset, a plaintext which satisfies all the criteria in the same round (round 4 is chosen), under the constraint that *the bytes satisfying these conditions are non-diagonal*, is found. By changing the diagonal values in the intermediate state, the semi-fixed plaintexts are generated. Based on this semi-fixed dataset, TVLA results using up to 3rd order statistics is computed [102].

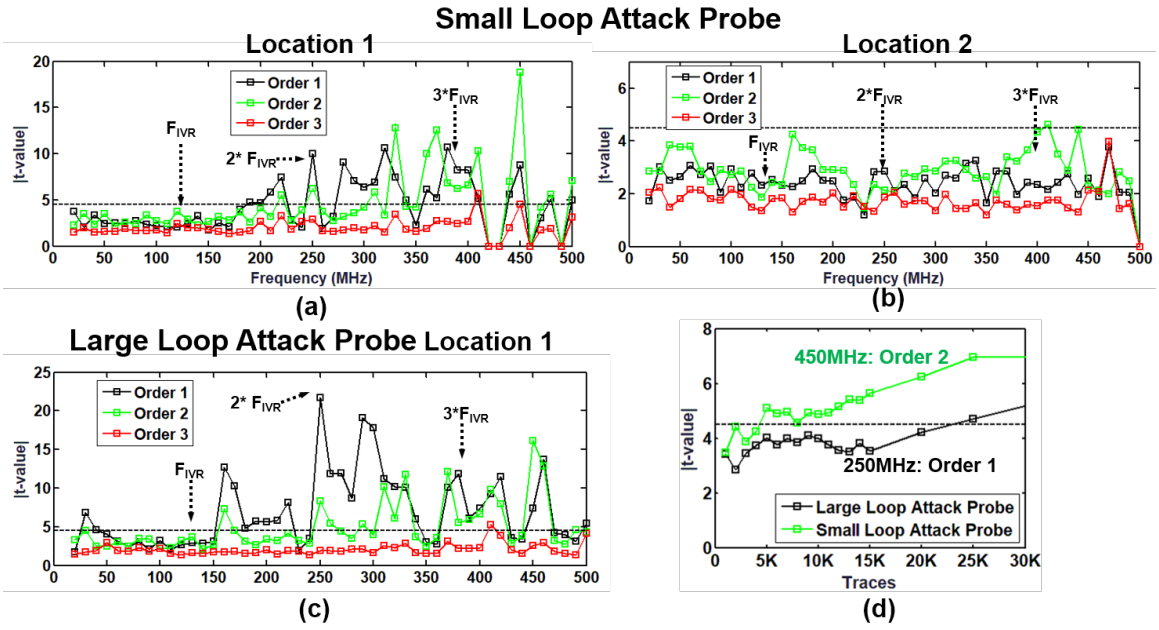

Figure 7.15: TVLA with AES powered the IVR without loop randomization at (a,b) two locations for the small loop probe and (c) the large loop. (d) Peak t-value against traces used.

AES Engine Supplied By the Off-Chip Voltage Regulator

We start with the AES engine supplied by the off-chip LDO. Signatures are captured for both the attack probes placed in location 1 which is the middle of the chip. Signatures captured by each of the probes show t-value more than 4.5, clearly showing that the EM signature contains leakage (Figure 7.14). The minimum number of traces needed to cross a t-value of 4.5 was 2K for both the probes. This experiment clearly shows that the unprotected AES has significant EM information leakage. We note that the component at the IVR frequency is easily filtered out by the post-processing step 7.4.2 clearly showing that having a strong EM radiator near the encryption engine isn't effective.

AES engine supplied by the IVR without randomization

Next the AES is powered with a baseline configuration of the IVR i.e. without the control-loop randomization. Although the signatures at location 1 for the small loop probe had no distinguishable AES part, TVLA shows leakage at frequencies higher than 200MHz. However, the same probe placed at location 2 i.e closer to the filter inductance shows weak leakage at higher frequency. The possible explanation of this behavior is that the obfuscation due to the EM signature from the IVR clock is smaller at location 1 due to the distance of the probe from the bondwires. Another interesting observation is that the 2nd order TVLA yield higher t-value than the first order. As the captured EM signatures are the result of a complex interaction between the AES and the IVR EM emission, higher order statistics shows better efficiency.

For the large loop attack probe, leakage is observed at the filter band at the AES_{CLK} as well as the IVR_{CLK} and its harmonics. Although the gain of the antenna loop drops significantly after 100MHz as shown in Figure 7.15, the larger loop area helps to pick up signatures at higher frequency successfully, leading to TVLA leakage.

We also characterized the minimum number of traces to cross the threshold of 4.5 for each probe at the frequency band and TVLA order which showed highest leakage. The smaller loop needs only 2.5K traces to cross the 4.5 threshold using a 2nd order TVLA. This is marginally better than the standalone AES scenario and clearly shows that even after the mutual modulation of the AES and the IVR frequencies, the obfuscation by the IVR has little effect. One possible reason can also be the placement of the probe away from the inductance. The larger loop requires 20K samples to cross a 4.5 threshold. These results are consistent with the observation of [64] which found that the baseline IVR design shows leakage in power signatures.

AES engine supplied by the IVR with LR active We present the results from the smaller loop attack probe as it was more vulnerable without LR than the larger loop probe. Figure 7.16 shows the time domain waveform of the captured signature with a small loop

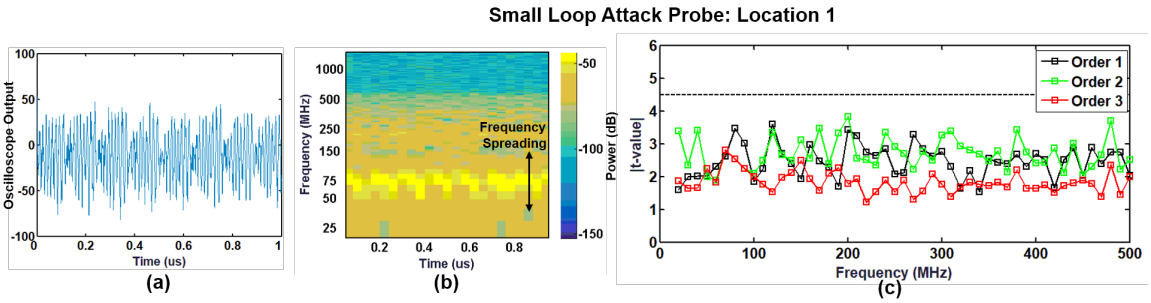

Figure 7.16: Signatures with IVR loop randomization turned on (a) time and (b) spectrogram. (c) TVLA across different frequency bands and different order with 500K traces

attack probe at location 1 and the corresponding spectral response when the randomization is enabled in the IVR control loop. As the random delay inserted into the control loop is controlled by a maximal length LFSR, the time domain voltage waveform shows a periodicity dictated by the length of the LFSR as well as control loop response based on the IVRs controller structure. This achieves the same effect of frequency spreading or frequency dithering with an added degree of randomness. No leakage was observed in the TVLA tests. This result indicates that randomization in the loop affects the EM signature captured from the AES engine even when the probe is placed right on top of the AES engine.

7.4.4 CPA Results

The power-model for CPA is chosen to be the hamming distance between the outputs of the 9th and the 10th round of the AES. Figure 7.17 shows the results of CPA on the AES Engine supplied by the off-chip VRM. A successful CPA is observed after using 40K traces. The corresponding MTD plot is also shown. The MTD using probe 2 is 30K (4th Byte is revealed).

CPA was also performed on the AES engine supplied by the IVR with randomization enabled. As the rounds of the IVR was not visible, we performed CPA across different frequency bands as described earlier with a sliding window that covers the entire encryption

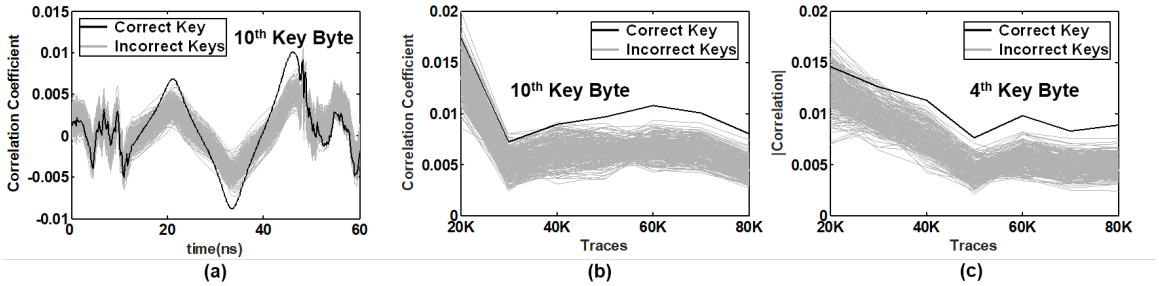

Figure 7.17: CPA on AES powered with the external VRM for 100K traces (a) Correlation against time for byte 10 (b,c) Correlation vs used traces for two bytes

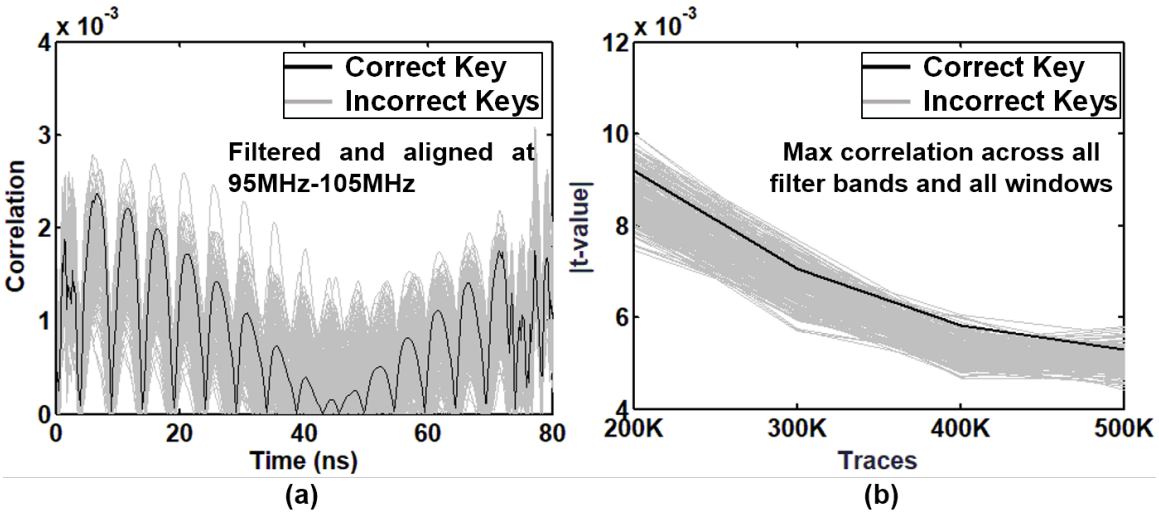

Figure 7.18: CPA on AES powered with the IVR (loop randomization turned on) attacking 10th key byte (a) a sample correlation-against-time plot after post-processing (b) MTD plot

period. This ensures that even if the leakage is present in the EM waveform with a time lag, it will get captured. No successful attack was observed with 500K traces across all bands and all windows (Figure 7.18).

7.5 Summary

This chapter demonstrates the potential of exploiting fully integrated inductive IVRs for improving EMSCA resistance, supported with measurement results from a test-chip with bond-wire based inductive IVR. Forensic EM probes with fine resolution is used to characterize the EM leakage from the package pins. The encryption engines are still vulnerable if a forensic probe is used in a lab environment and placed close to the AES engine. Two attack probes with different antenna dimensions are used to mimic a practical SCA scenario. Without randomizing the IVR loop, similar results to PSCA were obtained: TVLA shows signs of information leakage, however no successful CPA was observed. When the control loop is randomized using LR, TVLA shows no information leakage as well as no successful CPA was observed. The results show the potential for using inductive IVR as a common solution to improve power and EM side channel resistance, with LR effective in improving leakage for both these side channels.

CHAPTER 8
CONCLUSION AND FUTURE WORK

The energy-efficiency and security needs in computing systems, ranging from high performance processors to low-power devices are steadily increasing. This thesis details design and characterization of a fully integrated inductive voltage regulator, a block primarily used for improvement in energy efficiency, on improving power and EM side channel resistance of encryption engines. The low area/power/performance overhead of the proposed security-aware design changes in an inductive IVR and improvement in both power and EM side channel resistance of a 128-bit AES engine without any algorithmic or logical modification, make the proposed techniques attractive for implementation. In this chapter, we walk through a summary of the main contributions of this thesis in Section 8.1. We conclude by examining future research directions in Section 8.2.

8.1 Dissertation Summary

This thesis starts with identifying different transformations in an inductive IVR that modifies the load current signatures to generate the measured current signatures. **Chapter 3** demonstrates through a simulation framework that although an inductive IVR reduces correlation between the load current signatures and the input current signatures, correlation is not a useful metric to quantify PSCA resistance at the IVR input current signature, which shows a successful CPA for an illustrative design even though its correlation with the load current signature is low. Chapter 3 concludes that IVR can be used to improve CPA resistance of an AES engine (16x improvement in MTD) and the improvement is not vulnerable to a frequency domain CPA or a load-current-reconstruction based attack. However the fact that the IVR input current shows a successful CPA with 4000 current traces clearly indicates a strong data dependency at IVR input signatures.

Simulation based results might underestimate or overestimate the improvement in PSCA, particularly because the protection is not achieved through an algorithmic modification in the AES design and rather relies on different IVR transformations. Therefore, it is extremely crucial to validate the improvement in PSCA resistance through a hardware prototype. **Chapter 4** identifies the design issues of integrated inductive VRs in digital processes and details measurement results of an all-digital architecture of an inductive IVR using package bondwires as inductances, implemented in 130nm CMOS process. The designed controller architecture along with a transient assist scheme achieves a 2.9V/us voltage ramp rate for power-state transients and 71% peak power efficiency. **Chapter 5** characterizes the PSCA resistance at the input of the implemented IVR design for two different architectures of an AES engine: HP-AES suited for a high performance processor and LP-AES suited for a low-power application. The IVR input signatures show leakage in TVLA tests for both these designs. The CPA results show only a 1.5x improvement in MTD for a LP-AES whereas HP-AES shows a $\geq$20x improvement in MTD. These results support the observations made in Chapter 3 that an IVR improves the MTD of an AES engine, however still leaks information. This motivates the need for a security aware IVR design.

Chapter 6 introduces a security aware all-digital block called loop randomizer for modifying the IVR transformations through randomization of the control loop. The IVR maintains its stability when LR is activated and incurs a low area/power/performance overheads. The overheads however, can easily be justified with $\geq$20x and $\geq$100x improvement in CPA MTD for HP-AES and LP-AES respectively (no successful CPA for both AES designs with 100,000 traces), complete suppression of leakage in TVLA tests with 100,000 traces and ease of integration into the existing commercial and academic IVR designs.

Chapter 7 shows that the presence of an inductance in an inductive IVR can be exploited for improving EMSCA resistance as well. A characterization with EM probes with different resolutions show TVLA leakage in EM signatures from a baseline IVR configuration (without LR) for a HP-AES. Although no successful CPA was observed on 500,000

measurements from the baseline IVR-AES system (compared to a successful CPA with 40,000 measurements for the standalone AES), the presence of TVLA leakages indicates the need for a security aware design for EMSCA prevention. However, EM measurements, with the proposed loop-randomization activated, suppresses the TVLA leakage as well as prevents a successful CPA with 500,000 traces. The results suggest that a security-aware IVR design can be effective for improving resistance to both power and EM SCA.

8.2 Future Directions

Improving side-channel-resistance using energy efficient design techniques is a rich topic of research. It has been shown in this thesis that a security aware inductive IVR design, primarily meant for improving energy efficiency, can improve both power and EM side channel resistance. This thesis, along with few other recently published works [103, 104, 105] open up a new direction of research where circuit techniques for energy-efficiency can be used for improvement in side channel resistance.

Usage of integrated inductance: The fabricated chip uses bondwires as inductance as the fabrication technology does not support a high density on-chip inductance. As the bondwires are not spatially close to the placement of the AES engine, the AES design might be vulnerable to fine grain EM scanning of the die. However the maturing technology of inductance integration promises higher inductance density at a form factor similar to the dimensions of the physical design of the encryption blocks. Therefore a physical proximity of the encryption engine and the inductor can be more effective in masking the encryption signatures with the stronger signature from the inductor and needs to be verified using a hardware prototype. Moreover, unlike the commercial processors featuring inductive IVRs where both terminals of the inductance are also exposed, an integrated inductance promises electrical isolation of the inductor nodes and maintains the physical integrity of the system.

Instruction Profiling: Side channel attacks are not only limited to extracting key from encryption engines, but also used in profiling assembly level instructions from embedded

systems as demonstrated in [106, 107]. Profiling instructions from a hardware platform can be used for reverse engineering of code, and can lead to IP theft of embedded software. Typically an instruction profiling involves multiple side channel measurements of a single instruction executed with different values. The asynchronous relationship between the IVR clock and the digital clock again can be useful making profiling significantly harder.

New Attack Mode: LR is shown to be effective against existing statistical tests like CPA and TVLA (higher order TVLA for EMSCA). Other randomization based techniques like use of random fast voltage dithering in [105] have been recently proposed. The future research can focus on trying to find new attack modes for breaking any protection achieved through randomization of control loop or other elements in power delivery. For existing attack methods like CPA, alternative power-models which take into account the IVR transformations also needs to be investigated.

Public Key Cryptography: Public key ciphers are vulnerable to both power and EM SCA as demonstrated in [11, 10]. However, attacks are carried out at a much lower frequency as leakage corresponding to higher level instructions like addition and multiplication are exploited. Therefore the frequency of interest in such attacks is $\sim$100KHz-2MHz. The presented high frequency IVR with loop randomization might not be effective in hiding these side channel signatures. However, insights from the experiments suggest that any technique which causes the side channel spectrum to spread over the frequency of interest can help in improving the SCA resistance. Using the existing LR block with lower clock frequency, a slower dithering of the IVR switching frequency, or use of a pulse frequency modulation mode of operation can be investigated for the same purpose.

Appendices

APPENDIX A

ABBREVIATIONS

ADC	Analog-to-Digital Converter
AES	Advanced Encryption Standard
CCM	Continuous Conduction Mode
CPA	Correlation Power Analysis
CTF	Correlation Transfer Function
DPWM	Digital Pulse-Width-Modulator
DCM	Discontinuous Conduction Mode
EMSCA	Electromagnetic Side-Channel-Attack
FIVR	Fully Integrated Inductive Voltage Regulator
HD	Hamming Distance
HP-AES	High Performance AES Architecture
IVR	Integrated Voltage Regulator
LCO	Limit Cycle Oscillation
LDO	Low Dropout Regulator
LP-AES	Low-Power AES Architecture
LR	Loop Randomization
MTD	Measurement-to-disclosure
PID	Proportional-Integral-Derivative
PSCA	Power Side-Channel-Attack
PM	Phase-Margin
RTA	Resistive-Transient-Assist
RTF	Reverse-Transfer-Function

SCVR Switched-Capacitor based Voltage Regulator

SCA Side-Channel-Attack

SFOM Stability Figure-of-Merit

TVLA Test Vector Leakage Assessment

UGF Unity-Gain-Bandwidth

VR/VRM Voltage-Regulator (Module)

REFERENCES

[1] P. Hammarlund, A. J. Martinez, A. A. Bajwa, D. L. Hill, E. Hallnor, H. Jiang, M. Dixon, M. Derr, M. Hunsaker, R. Kumar, R. B. Osborne, R. Rajwar, R. Singhal, R. D. Sa, R. Chappell, S. Kaushik, S. Chennupaty, S. Jourdan, S. Gunther, T. Piazza, and T. Burton, "Haswell: the fourth-generation intel core processor," *IEEE Micro*, vol. 34, no. 2, pp. 6–20, 2014.

[2] C. F. Webb, "Ibm z10: the next-generation mainframe microprocessor," *IEEE Micro*, vol. 28, no. 2, pp. 19–29, 2008.

[3] A. Krishna, T. Heil, N. Lindberg, F. Toussi, and S. VanderWiel, "Hardware acceleration in the ibm poweren processor: architecture and performance," in *Proceedings of the 21st international conference on Parallel architectures and compilation techniques*, ACM, pp. 389–400, ISBN: 1450311822.

[4] R. Hou, L. Zhang, M. C. Huang, K. Wang, H. Franke, Y. Ge, and X. Chang, "Efficient data streaming with on-chip accelerators: opportunities and challenges," in *High Performance Computer Architecture (HPCA), 2011 IEEE 17th International Symposium on*, IEEE, pp. 312–320, ISBN: 1424494354.

[5] V. Costan and S. Devadas, "Intel sgx explained," *IACR Cryptology ePrint Archive*, vol. 2016, p. 86, 2016.

[6] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in cryptologyCRYPTO99*, Springer, pp. 789–789.

[7] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, pp. 16–29.

[8] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[9] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): measures and counter-measures for smart cards," *Smart Card Programming and Security*, pp. 200–210, 2001.

[10] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from pcs using a radio: cheap electromagnetic attacks on windowed exponentiation," in *Inter-*

national Workshop on Cryptographic Hardware and Embedded Systems, Springer, pp. 207–228.

[11] ——, "Ecdh key-extraction via low-bandwidth electromagnetic attacks on pcs," in *Cryptographers Track at the RSA Conference*, Springer, pp. 219–235.

[12] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em sidechannel(s)," in *Cryptographic Hardware and Embedded Systems - CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 1315, 2002 Revised Papers*, B. S. Kaliski, . K. Ko, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45, ISBN: 978-3-540-36400-9.

[13] O. Choudary and M. G. Kuhn, "Efficient template attacks," in *Smart Card Research and Advanced Applications: 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers*, A. Francillon and P. Rohatgi, Eds. Cham: Springer International Publishing, 2014, pp. 253–270, ISBN: 978-3-319-08302-5.

[14] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Cryptographic Hardware and Embedded Systems CHES 2000: Second International Workshop Worcester, MA, USA, August 1718, 2000 Proceedings*, . K. Ko and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 71–77, ISBN: 978-3-540-44499-2.

[15] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An on-chip signal suppression countermeasure to power analysis attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 3, pp. 179–189, 2004.

[16] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, IEEE Computer Society, p. 10 246, ISBN: 0769520855.

[17] J. Blmer, J. Guajardo, and V. Krummel, "Provably secure masking of aes," in *International Workshop on Selected Areas in Cryptography*, Springer, pp. 69–83.

[18] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: dpa-resistance without routing constraints," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, pp. 172–186.

[19] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype ic with wddl and differential routing dpa resistance assessment," in *Cryptographic Hardware and Embedded Systems CHES 2005: 7th International Workshop, Edinburgh, UK, August 29 September 1, 2005. Proceedings*, J. R. Rao

and B. Sunar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 354–365, ISBN: 978-3-540-31940-5.

[20] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *CHES*, vol. 4249, Springer, pp. 232–241.

[21] C. Herbst, E. Oswald, and S. Mangard, "An aes smart card implementation resistant to power analysis attacks," in *ACNS*, vol. 3989, Springer, pp. 239–252.

[22] T. Plos, M. Hutter, and C. Herbst, "Enhancing side-channel analysis with low-cost shielding techniques," in *Proceedings of Austrochip*, 2008, pp. 90–95.

[23] D. D. Hwang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Aes-based security coprocessor ic in 0.18um cmos with resistance to differential power analysis side-channel attacks," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, 2006.

[24] V. Telandro, E. Kussener, A. Malherbe, and H. Barthelemy, "On-chip voltage regulator protecting against power analysis attacks," in *2006 49th IEEE International Midwest Symposium on Circuits and Systems*, vol. 2, pp. 507–511, ISBN: 1548-3746.

[25] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 7, pp. 1197–1208, 2006.

[26] M. Hutter, S. Mangard, and M. Feldhofer, "Power and em attacks on passive 13.56mhz rfid devices," in *Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 320–333, ISBN: 978-3-540-74735-2.

[27] J.-S. Coron and I. Kizhvatov, "An efficient method for random delay generation in embedded software," in *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, 2009, pp. 156–170.

[28] J. P. Kaps and R. Velegalati, "Dpa resistant aes on fpga using partial ddl," in *2010 18th IEEE Annual International Symposium on Field-Programmable Custom Computing Machines*, pp. 273–280.

[29] H. Kim, S. Hong, and J. Lim, "A fast and provably secure higher-order masking of aes s-box," in *Cryptographic Hardware and Embedded Systems CHES 2011: 13th International Workshop, Nara, Japan, September 28 October 1, 2011. Proceedings*, B. Preneel and T. Takagi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 95–107, ISBN: 978-3-642-23951-9.

[30] 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, 2010.

[31] S. Das, C. Tokunaga, S. Pant, W. H. Ma, S. Kalaiselvan, K. Lai, D. M. Bull, and D. T. Blaauw, "Razorii: in situ error detection and correction for pvt and ser tolerance," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 1, pp. 32–48, 2009.

[32] K. Chae, S. Mukhopadhyay, C.-H. Lee, and J. Laskar, "A dynamic timing control technique utilizing time borrowing and clock stretching," in *Custom Integrated Circuits Conference (CICC), 2010 IEEE*, IEEE, pp. 1–4, ISBN: 1424457602.

[33] M. Cho, S. T. Kim, C. Tokunaga, C. Augustine, J. P. Kulkarni, K. Ravichandran, J. W. Tschanz, M. M. Khellah, and V. De, "Postsilicon voltage guard-band reduction in a 22 nm graphics execution core using adaptive voltage scaling and dynamic power gating," *IEEE Journal of Solid-State Circuits*, vol. 52, no. 1, pp. 50–63, 2017.

[34] D. Bol, J. De Vos, C. Hocquet, F. Botman, F. Durvaux, S. Boyd, D. Flandre, and J.-D. Legat, "Sleepwalker: a 25-mhz 0.4-v sub-microcontroller in 65-nm lp/gp cmos for low-carbon wireless sensor nodes," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 1, pp. 20–32, 2013.

[35] B. Keller, M. Cochet, B. Zimmer, Y. Lee, M. Blagojevic, J. Kwak, A. Puggelli, S. Bailey, P. F. Chiu, P. Dabbelt, C. Schmidt, E. Alon, K. Asanovi, and B. Nikoli, "Sub-microsecond adaptive voltage scaling in a 28nm fd-soi processor soc," in *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, pp. 269–272.

[36] S. T. Kim, Y. C. Shih, K. Mazumdar, R. Jain, J. F. Ryan, C. Tokunaga, C. Augustine, J. P. Kulkarni, K. Ravichandran, J. W. Tschanz, M. M. Khellah, and V. De, "Enabling wide autonomous dvfs in a 22 nm graphics execution core using a digitally controlled fully integrated voltage regulator," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 1, pp. 18–30, 2016.

[37] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact rijndael hardware architecture with s-box optimization," in *Asiacrypt*, vol. 2248, Springer, pp. 239–254.

[38] S. Mathew, S. Satpathy, V. Suresh, M. Anders, H. Kaul, A. Agarwal, S. Hsu, G. Chen, and R. Krishnamurthy, "340 mv1.1 v, 289 gbps/w, 2090-gate nanoaes hardware accelerator with area-optimized encrypt/decrypt gf (2 4) 2 polynomials in 22 nm tri-gate cmos," *IEEE Journal of Solid-State Circuits*, vol. 50, no. 4, pp. 1048–1058, 2015.

[39] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "Aes implementation on a grain of sand," *IEE Proceedings-Information Security*, vol. 152, no. 1, pp. 13–20, 2005.

[40] A. Singh, M. Kar, J. H. Ko, and S. Mukhopadhyay, "Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators," in *2015 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, pp. 134–139.

[41] E. A. Burton, G. Schrom, F. Paillet, J. Douglas, W. J. Lambert, K. Radhakrishnan, and M. J. Hill, "Fivr - fully integrated voltage regulators on 4th generation intel core socs," in *2014 IEEE Applied Power Electronics Conference and Exposition - APEC 2014*, pp. 432–439, ISBN: 1048-2334.

[42] R. Jain, B. M. Geuskens, S. T. Kim, M. M. Khellah, J. Kulkarni, J. W. Tschanz, and V. De, "A 0.45-1 v fully-integrated distributed switched capacitor dc-dc converter with high density mim capacitor in 22 nm tri-gate cmos," *IEEE Journal of Solid-State Circuits*, vol. 49, no. 4, pp. 917–927, 2014.

[43] M. Kar, A. Singh, A. Rajan, V. De, and S. Mukhopadhyay, "An integrated inductive vr with a 250mhz all-digital multisampled compensator and on-chip auto-tuning of coefficients in 130nm cmos," in *ESSCIRC Conference 2016: 42nd European Solid-State Circuits Conference*, pp. 453–456.

[44] B. Sinharoy, J. Van Norstrand, R. J. Eickemeyer, H. Q. Le, J. Leenstra, D. Q. Nguyen, B Konigsburg, K Ward, M. Brown, and J. E. Moreira, "Ibm power8 processor core microarchitecture," *IBM Journal of Research and Development*, vol. 59, no. 1, 2: 1–2: 21, 2015.

[45] Z. Toprak-Deniz, M. Sperling, J. Bulzacchelli, G. Still, R. Kruse, S. Kim, D. Boerstler, T. Gloekler, R. Robertazzi, and K. Stawiasz, "5.2 distributed system of digitally controlled microregulators enabling per-core dvfs for the power8 tm microprocessor," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International*, IEEE, pp. 98–99, ISBN: 1479909203.

[46] S. B. Nasir, S. Gangopadhyay, and A. Raychowdhury, "5.6 a 0.13um fully digital low-dropout regulator with adaptive control and reduced dynamic stability for ultra-wide dynamic range," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, pp. 1–3, ISBN: 0193-6530.

[47] E. J. Fluhr, S. Baumgartner, D. Boerstler, J. F. Bulzacchelli, T. Diemoz, D. Dreps, G. English, J. Friedrich, A. Gattiker, and T. Gloekler, "The 12-core power8 processor with 7.6 tb/s io bandwidth, integrated voltage regulation, and resonant clocking," *IEEE Journal of Solid-State Circuits*, vol. 50, no. 1, pp. 10–23, 2015.

[48] R. J. Milliken, J. Silva-Martinez, and E. Sanchez-Sinencio, "Full on-chip cmos low-dropout voltage regulator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 54, no. 9, pp. 1879–1890, 2007.

[49] Y. Ahn, H. Nam, and J. Roh, "A 50-mhz fully integrated low-swing buck converter using packaging inductors," *IEEE Transactions on Power Electronics*, vol. 27, no. 10, pp. 4347–4356, 2012.

[50] H. K. Krishnamurthy, V. A. Vaidya, P. Kumar, G. E. Matthew, S. Weng, B. Thiruvengadam, W. Proefrock, K. Ravichandran, and V. De, "A 500 mhz, 68buck voltage regulator on 22nm tri-gate cmos," in *2014 Symposium on VLSI Circuits Digest of Technical Papers*, pp. 1–2, ISBN: 2158-5601.

[51] M. Lee, Y. Choi, and J. Kim, "A 500-mhz, 0.76-w/mm power density and 76.2fully integrated digital buck converter in 65-nm cmos," *IEEE Transactions on Industry Applications*, vol. 52, no. 4, pp. 3315–3323, 2016.

[52] C. Huang and P. K. Mok, "An 84.7integrated buck converter with precise dcm operation and enhanced light-load efficiency," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 11, pp. 2595–2607, 2013.

[53] C. Huang and P. K. T. Mok, "A 100 mhz 82.4fully-integrated buck converter with flying capacitor for area reduction," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 12, pp. 2977–2988, 2013.

[54] P. Hazucha, G. Schrom, H. Jaehong, B. A. Bloechel, P. Hack, G. E. Dermer, S. Narendra, D. Gardner, T. Karnik, V. De, and S. Borkar, "A 233-mhz 80utilizing air-core inductors on package," *IEEE Journal of Solid-State Circuits*, vol. 40, no. 4, pp. 838–845, 2005.

[55] H. K. Krishnamurthy, V. Vaidya, S. Weng, K. Ravichandran, P. Kumar, S. Kim, R. Jain, G. Matthew, J. Tschanz, and V. De, "20.1 a digitally controlled fully integrated voltage regulator with on-die solenoid inductor with planar magnetic core in 14nm tri-gate cmos," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 336–337.

[56] H.-P. Le, M. Seeman, S. R. Sanders, V. Sathe, S. Naffziger, and E. Alon, "A 32nm fully integrated reconfigurable switched-capacitor dc-dc converter delivering 0.55 w/mm2 at 81 efficiency," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2010 IEEE International*, IEEE, pp. 210–211, ISBN: 1424460360.

[57] T. M. Andersen, F. Krismer, J. W. Kolar, T. Toifl, C. Menolfi, L. Kull, T. Morf, M. Kossel, M. Brandli, and P. Buchmann, "4.7 a sub-ns response on-chip switched-capacitor dc-dc voltage regulator delivering 3.7 w/mm 2 at 90capacitors in 32nm

soi cmos," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International*, IEEE, pp. 90–91, ISBN: 1479909203.

[58] S. S. Kudva and R. Harjani, "Fully-integrated on-chip dc-dc converter with a 450x output range," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 8, pp. 1940–1951, 2011.

[59] N. Sturcken, E. O. Sullivan, N. Wang, P. Herget, B. Webb, L. Romankiw, M. Petracca, R. Davies, R. Fontana, G. Decad, I. Kymissis, A. Peterchev, L. Carloni, W. Gallagher, and K. Shepard, "A 2.5d integrated voltage regulator using coupled-magnetic-core inductors on silicon interposer delivering 10.8a/mm¡sup¿2¡/sup¿," in *2012 IEEE International Solid-State Circuits Conference*, pp. 400–402, ISBN: 0193-6530.

[60] N. Sturcken, R. Davies, H. Wu, M. Lekas, K. Shepard, K. W. Cheng, C. C. Chen, Y. S. Su, C. Y. Tsai, K. D. Wu, J. Y. Wu, Y. C. Wang, K. C. Liu, C. C. Hsu, C. L. Chang, W. C. Hua, and A. Kalnitsky, "Magnetic thin-film inductors for monolithic integration with cmos," in *2015 IEEE International Electron Devices Meeting (IEDM)*, pp. 11.4.1–11.4.4.

[61] M. Kar, A. Singh, A. Rajan, V. De, and S. Mukhopadhyay, "An all-digital fully integrated inductive buck regulator with a 250-mhz multi-sampled compensator and a lightweight auto-tuner in 130-nm cmos," *IEEE Journal of Solid-State Circuits*, 2017.

[62] S Mueller, K. Ahmed, A Singh, A. Davis, S Mukhopadyay, M Swaminathan, Y Mano, Y Wang, J Wong, and S Bharathi, "Design of high efficiency integrated voltage regulators with embedded magnetic core inductors," in *Electronic Components and Technology Conference (ECTC), 2016 IEEE 66th*, IEEE, pp. 566–573, ISBN: 1509012044.

[63] R. Anderson, M. Bond, J. Clulow, and S. Skorobogatov, "Cryptographic processors-a survey," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 357–369, 2006.

[64] 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)*, pp. 142–143.

[65] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip," in *Cryptographic Hardware and Embedded Systems – CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings*, T. Gneysu and H. Handschuh, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 620–640, ISBN: 978-3-662-48324-4.

[66] J. A. Ambrose, S. Parameswaran, and A. Ignjatovic, "Mute-aes: a multiprocessor architecture to prevent power analysis based side channel attack of the aes algorithm," in *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, IEEE Press, pp. 678–684, ISBN: 1424428203.

[67] M. Rivain and E. Prouff, "Provably secure higher-order masking of aes," *Cryptographic Hardware and Embedded Systems, CHES 2010*, pp. 413–427, 2010.

[68] M. Nassar, Y. Souissi, S. Guilley, and J.-L. Danger, "Rsm: a small and fast countermeasure for aes, secure against 1st and 2nd-order zero-offset scas," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2012*, IEEE, pp. 1173–1178, ISBN: 1457721457.

[69] M. Nassar, S. Bhasin, J.-L. Danger, G. Duc, and S. Guilley, "Bcdl: a high speed balanced dpl for fpga with global precharge and no early evaluation," in *Proceedings of the Conference on Design, Automation and Test in Europe*, European Design and Automation Association, pp. 849–854, ISBN: 3981080165.

[70] S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32 ghz high-throughput charge-recovery aes core with resistance to dpa attacks," in *VLSI Circuits (VLSI Circuits), 2015 Symposium on*, IEEE, pp. C246–C247, ISBN: 4863485026.

[71] Z. Chen and Y. Zhou, "Dual-rail random switching logic: a countermeasure to reduce side channel leakage," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, pp. 242–254.

[72] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style mdpl on a prototype chip," in *Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 81–94, ISBN: 978-3-540-74735-2.

[73] T. Gneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Cryptographic Hardware and Embedded Systems CHES 2011: 13th International Workshop, Nara, Japan, September 28 October 1, 2011. Proceedings*, B. Preneel and T. Takagi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 33–48, ISBN: 978-3-642-23951-9.

[74] W. Xinmu, Y. Wen, D. B. Roy, S. Narasimhan, Z. Yu, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, "Role of power grid in side channel attack and power-grid-aware secure design," in *2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–9, ISBN: 0738-100X.

[75] ——, "Role of power grid in side channel attack and power-grid-aware secure design," in *2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–9, ISBN: 0738-100X.

[76] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," *arXiv preprint arXiv:1703.10328*, 2017.

[77] 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)*, pp. 145–148.

[78] W. Yu and S. Kse, "A voltage regulator-assisted lightweight aes implementation against dpa attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 8, pp. 1152–1163, 2016.

[79] S. Saab, A. Leiserson, and M. Tunstall, "Key extraction from the primary side of a switched-mode power supply," in *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, pp. 1–7.

[80] P. Rohatgi, "Electromagnetic attacks and countermeasures," in *Cryptographic Engineering*, . K. Ko, Ed. Boston, MA: Springer US, 2009, pp. 407–430, ISBN: 978-0-387-71817-0.

[81] P. Maistri, S. Tiran, P. Maurine, I. Koren, and R. Leveugle, "Countermeasures against em analysis for a secured fpga-based aes implementation," in *Reconfigurable Computing and FPGAs (ReConFig), 2013 International Conference on*, IEEE, pp. 1–6, ISBN: 1479920797.

[82] M. Doulcier-Verdier, J.-M. Dutertre, J. Fournier, J.-B. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant aes circuit working on duplicated complemented values," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2011 IEEE International*, IEEE, pp. 274–276, ISBN: 1612843026.

[83] M. Yamaguchi, H. Toriduka, S. Kobayashi, T. Sugawara, N. Hommaa, A. Satoh, and T. Aoki, "Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic lsi from electromagnetic analysis," in *2010 IEEE International Symposium on Electromagnetic Compatibility*, pp. 103–108, ISBN: 2158-110X.

[84] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, IEEE, 2015, pp. 1–6.

[85] "Introduction to matlab/simulink for switched-mode power converters,"

[86] M. Kar, D. Lie, M Wolf, V. De, and S. Mukhopadhyay, "Impact of inductive integrated voltage regulator on the power attack vulnerability of encryption engines: a simulation study," in *Custom Integrated Circuits Conference (CICC), 2014 IEEE Proceedings of the*, IEEE, pp. 1–4, ISBN: 1479932868.

[87] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines.," in *ISLPED*, 2016, pp. 130–135.

[88] S. Arora, D. K. Su, and B. A. Wooley, "A compact 120-mhz 1.8v/1.2v dual-output dc-dc converter with digital control," in *Proceedings of the IEEE 2013 Custom Integrated Circuits Conference*, pp. 1–4, ISBN: 0886-5930.

[89] H. Fujita, "A single-phase active filter using an h-bridge pwm converter with a sampling frequency quadruple of the switching frequency," *IEEE Transactions on Power Electronics*, vol. 24, no. 4, pp. 934–941, 2009.

[90] L. Corradini, P. Mattavelli, E. Tedeschi, and D. Trevisan, "High-bandwidth multisampled digitally controlled dc-dc converters using ripple compensation," *IEEE Transactions on Industrial Electronics*, vol. 55, no. 4, pp. 1501–1508, 2008.

[91] M. Shirazi, R. Zane, and D. Maksimovic, "An autotuning digital controller for dc-dc power converters based on online frequency-response measurement," *IEEE Transactions on Power Electronics*, vol. 24, no. 11, pp. 2578–2588, 2009.

[92] J. A. A. Qahouq and V. Arikatla, "Online closed-loop autotuning digital controller for switching power converters," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 5, pp. 1747–1758, 2013.

[93] M. Kar, S. Carlo, H. Krishnamurthy, and S. Mukhopadhyay, "Impact of process variation in inductive integrated voltage regulator on delay and power of digital circuits," in *Low Power Electronics and Design (ISLPED), 2014 IEEE/ACM International Symposium on*, IEEE, pp. 227–232.

[94] Y. M. Tousi and E. Afshari, "A miniature 2 mw 4 bit 1.2 gs/s delay-line-based adc in 65 nm cmos," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 10, pp. 2312–2325, 2011.

[95] A. V. Peterchev and S. R. Sanders, "Quantization resolution and limit cycling in digitally controlled pwm converters," *IEEE Transactions on Power Electronics*, vol. 18, no. 1, pp. 301–308, 2003.

[96] E. J. Carlson, K. Strunz, and B. P. Otis, "A 20 mv input boost converter with efficient digital control for thermoelectric energy harvesting," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 4, pp. 741–750, 2010.

[97] N. Sturcken, M. Petracca, S. Warren, P. Mantovani, L. P. Carloni, A. V. Peterchev, and K. L. Shepard, "A switched-inductor integrated voltage regulator with nonlinear feedback and network-on-chip load in 45 nm soi," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 8, pp. 1935–1945, 2012.

[98] B. J. Gilbert Goodwill, J. Jaffe, and P. Rohatgi, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*.

[99] F. Debeer, M. Witteman, B. Gedrojc, and Y. Sheng, "Practical electro-magnetic analysis," in *Non-invasive Attack Testing Workshop NIAT, Nara: Todai-ji Cultural Center (Technical Programs)*.

[100] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," in *Cryptographic Hardware and Embedded SystemsCHES 2001*, Springer, pp. 251–261.

[101] 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 *Microarchitecture (MICRO), 2014 47th Annual IEEE/ACM International Symposium on*, IEEE, pp. 242–254, ISBN: 1479969982.

[102] T. Schneider and A. Moradi, "Leakage assessment methodology," in *International Workshop on Cryptographic Hardware and Embedded Systems*, Springer, pp. 495–513.

[103] M. Kar, A. Singh, A. Rajan, V. De, and S. Mukhopadhyay, "What does ultra low power requirements mean for side-channel secure cryptography?" In *Computer Design (ICCD), 2016 IEEE 34th International Conference on*, IEEE, 2016, pp. 686–689.

[104] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "(invited) low power requirements and side-channel protection of encryption engines: challenges and opportunities," in *ISLPED*, 2017.

[105] A Singh, M. Kar, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power side channel attack resistance of a 128-bit aes engine with random fast voltage dithering," in *ESSCIRC Conference 2017: 43nd European Solid-State Circuits Conference*.

[106] M. Msgna, K. Markantonakis, K. Mayes, X Huang, and J Zhou, "Precise instruction-level side channel profiling of embedded processors," in *ISPEC*, pp. 129–143.

[107] D. Strobel, F. Bache, D. Oswald, F. Schellenberg, and C. Paar, "Scandalee: a side-channel-based disassembler using local electromagnetic emanations," in *Design, Automation and Test in Europe Conference Exhibition (DATE), 2015*, IEEE, pp. 139–144, ISBN: 398153705X.