ENERGY-EFFICIENT AND SCA-RESISTANT CRYPTOGRAPHIC HARDWARE FOR IOT APPLICATIONS

A Dissertation
Presented to
The Academic Faculty

By

Arvind Singh

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Georgia Institute of Technology

Georgia Institute of Technology

August 2019

ENERGY-EFFICIENT AND SCA-RESISTANT CRYPTOGRAPHIC HARDWARE FOR IOT APPLICATIONS

Approved by:

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

Dr. Tushar Krishna
School of Electrical and Computer Engineering
Georgia Institute of Technology

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

Dr. Hyesoon Kim
School of Computer Science
Georgia Institute of Technology

Dr. Vivek De
Circuits Research Lab
Intel Labs

Date Approved: July 8, 2019

Look up at the stars and not down at your feet. Try to make sense of what you see, and wonder about what makes the universe exist. Be curious.

–Stephen Hawking

To my family.

ACKNOWLEDGEMENTS

I would like to express my most sincere gratitude towards my advisor, Professor Saibal Mukhopadhyay, for the support and encouragement he provided throughout my PhD. I'd like to thank him for believing in my abilities, even at times when my own confidence wavered. His persistent motivation and encouragement gave me strength to overcome difficulties, take up new challenges and to come up with innovative ideas, I will forever remain indebted to him. I could not have imagined having a better advisor and mentor for my Ph.D study, his advice on my research as well as on my career has been invaluable.

I'd also like to extend my thanks to dissertation committee members - Prof. Tushar Krishna, Prof. Raheem Beyah, Prof. Hyesoon Kim and Dr. Vivek De for their time, support, for their insightful comments and constructive feedback before and during the dissertation defence process which helped me a lot to improve the quality of my dissertation.

I am thankful to past members of the GREEN Lab, Dr. Amit Ranjan Trivedi, Dr. Boris Alexandrov, Dr. Sergio Carlo, Dr. Denny Lie, Dr. Wen Yueh, Dr. Khondker Z. Ahmed, Dr. Monodeep Kar, Dr. Jaeha Kung, Dr. Duckhwan Kim, Dr. Jong-HWan Ko, Dr. Md. Faisal Amir and Dr. Taesik Na, who mentored me and provided tremendous support to make PhD research less stressful and more fun. I'd especially like to thank Dr. Monodeep Kar for 3-long years of collaborative research and numerous discussions on multitude of research problems. I'd like to extend my sincere thanks to current members of GREEN Lab, Yun Long, Burhan, Chaitanya, Edward, Nikhil, Minah, Nihar, Priyabrata, Xueyuan, Nael, Arslan, Mandovi, Daehyun, who have been of immense help throughout the thesis work in countless ways, GREEN Lab wouldn't have been the same without them!

I'd like to acknowledge the support of my family, especially my parents who have raised me to be the person I am today. I would also like to thank my brothers Vinay and Amit and sister Kalpana for their love and support throughout the years and to my highschool teacher Mr. Manoj Dwivedi for his continued guidance, teachings and belief in

me. Most importantly, I'd like to thank my wife, Pratima, who partners with me to tackle every challenge life throws my way, she is equally responsible for all of my achievements. I want to thank her for all the unconditional love, for helping me to see the bright side of things and being always by my side which gave me the confidence that no matter how challenging my goals become, I am capable of achieving them with my persistence and her unwavering faith in me.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

The rapid growth in the number of devices connected to the network has transformed the computing paradigm in all walks of human life, from autonomous vehicles to healthcare, industrial and home automation. The internet of things (IoT) devices help in achieving higher energy-efficiency, accuracy, speed and faster design cycles compared to general purpose computing devices. Security and privacy of critical and sensitive data is a major challenge for all computing systems, however, these network-connected devices have been overlooked with respect to device-related security risks owing to lack of resources at IoT edge nodes. Moreover, encryption algorithms implemented in hardware on these devices to secure inter-device communication emit information about the key through physical side channels leading to research challenges in designing energy-efficient, compact and side channel attack (SCA) resistant cryptographic hardware for IoT applications. This thesis investigates alternative hardware architectures for SIMON for higher energy-efficiency and design of lightweight SCA countermeasures utilizing on-chip integrated power-management and clocking techniques.

We propose alternative hardware architectures for lightweight cipher SIMON, at bit-/round-level parallelism, implemented in ASIC and FPGA platforms. Round unrolling (round-level parallelism) not only improves the energy-efficiency at small area, power overheads but also increases SCA resistance with deeper diffusion of the key, reduced signal-to-noise ratio (SNR) and increased complexity in modeling true leakage. The optimized SIMON engine is applied to a low-power image sensor node to analyze the overheads for secured communication.

Power management and low-power techniques employed in modern high-performance and low-power systems for improved energy-efficiency modulate/modify power and electromagnetic (EM) side-channel leakage and therefore it is essential to understand their role in improving SCA resistance. We propose lightweight countermeasures utilizing on-chip

fully-integrated inductive voltage regulator (FIVR) and digital low-dropout (DLDO) regulator along-with all-digital clock modulation (ADCM) circuit to improve SCA resistance of SIMON and advanced encryption standard (AES) encryption engines.

A random fast voltage dithering (RFVD) scheme with FIVR and ADCM is developed to randomize side channel signatures to improve SCA resistance for the local supply node of the AES cores which is exposed outside for bondwire or package based inductors. To eliminate the need for large passives (L, C), a major drawback for FIVR, a side channel protection scheme is proposed using DLDO and ADCM circuits. DLDO transforms the encryption patterns when measured at the input supply node and therefore enhances the SCA resistance. Two additional circuit techniques, namely, switching noise injector (SNI) and random reference word (R-VREF) generator are proposed to induce more randomness. The proposed FIVR, DLDO, randomization circuits along with 128-bit AES and SIMON cores are prototyped in two testchips in 130nm CMOS process and SCA measurements demonstrate improved resistance with respect to test vector leakage assessment (TVLA) and correlation power and EM analysis (CPA & CEMA) attacks. Due to all-digital nature of the proposed circuits, they easily integrate into digital design flows and are scalable across process nodes. Additionally, the overheads associated with these circuits are minimal compared to existing SCA countermeasures.

CHAPTER 1
INTRODUCTION

The emergence of pervasive computing has led to exponential growth of IoT devices from smart homes to smart wearables and toys, smart healthcare, autonomous vehicles and industrial equipment [1, 2]. For remote monitoring and processing, most of these devices are connected to the internet communicating sensitive information over the insecure wireless channels requiring encryption and authentication protocols to ensure safety and confidentiality [3]. Even though these security protocols have been proven secure against bruteforce or cryptanalysis attacks, their hardware or software implementations leak certain information via physical and architectural side channels such as power consumption [4], electromagnetic (EM) emissions [5], timing [4], acoustic signals [6], speculative execution [7–9], cache timing [10] etc. Side channel attacks, considered to be one of the seven properties defined for the highly secure devices by Microsoft Researchers [11], are very critical for the security for the modern computing devices. These side channels are part of the hardware design itself and therefore are notoriously difficult to defeat.

Several side channel analysis (SCA) attacks have been demonstrated to extract secret key used during the security operations by exploiting data-dependent information leaked through power, EM, timing side channels [4, 5, 12]. Modern computing systems are built using digital gates and the current drawn by these gates when they switch is dependent on the input vectors. An adversary can exploit the correlation between measured current signature and the input vectors to reveal the secret key. Various statistical analysis methods are used to exploit this data dependency, namely, differential power analysis (DPA) [12], correlation power analysis (CPA) [13], and template attacks (TA) [14]. Several countermeasures [15–29] have been developed in past two decades to either mask or hide information leakage through these side channels. However, due to high development costs, the hardened

security protocols are only limited to high-cost or high-margin devices [11]. For example, ARM Cortex instruction set architecture (ISA) offers TrustZone technology where trusted and untrusted operations are executed in two different worlds, namely, secure and normal operatig systems (OS), simultaneously running on a single core. Similarly, Intel's x86 ISA defines Software Guard Extensions (SGX) instructions to increase the security of application code and data, offering more isolation and protection to the sensitive operations using secure enclaves.

IoT devices drive huge economic efficiencies, however, due to severe resource constraints and price-sensitivity, they are ill-prepared for the security challenges of internet connectivity, exposing consumers and society to the perils of device security and privacy failures. To incorporate appropriate security features on IoT edge nodes, several lightweight cryptographic algorithms and primitives are being considered with PRINCE [30], PRESENT, [31], CLEFIA [32], Keccak [33], Whirlpool [34] and SIMON/SPECK [35] being few of the recently proposed candidates for lightweight encryption and authentication protocols. SIMON, introduced by National Institute of Standards and Technology (NIST) and optimized for hardware implementations, is an attractive option as it has been reported to be most compact implementation among all candidates [36]. However, for battery-operated IoT devices, energy-efficiency is another aspect which must be considered along with area. Most compact implementations may not be the most energy-efficient due to various tradeoffs. Additionally, accelerated hardware implementations should also be considered to ensure cryptographic blocks not being the bottleneck for the whole system.

At the circuit and architecture level, several power management and low-power techniques exist to improve the system energy-efficiency as well as performance such as distributed on-chip voltage regulation, dynamic voltage scaling (DVS) [37], dynamic voltage and frequency scaling (DVFS) [38] and clock and power gating [39]. Integration of voltage regulation modules on-chip [39–41] provides very fast response to transient events and reduces the overheads associated with switching of power states and therefore facil-

itates fine-grain power management for multiple DVFS domains. Adaptive clocking is another technique which eliminates timing/supply margins under variations, therefore improving system performance or reducing the total power [42, 43]. These techniques modulate/modify power side-channel leakage and therefore it is essential to understand their interaction with side-channel security of underlying cryptographic hardware. DVFS enabled with external VR and clock source has been demonstrated to improve SCA resistance [44, 45]. However, due to slower voltage-frequency transitions, there is a limited randomization that can be introduced, specifically for hardware accelerated encyrption engines. Impact of FIVR and switched capacitor voltage regulators (SCVR) has been previously investigated [46–52] and demonstrated to improve the SCA resistance at the input supply node of the chip. However, on-chip integration of large passives (L, C) is very expensive and generally not desired for low-cost applications. Consequently, for on-package or printed circuit board (PCB) based inductors/capacitors where local supply node for the encryption engine is exposed outside, these countermeasures provide negligible or little SCA resistance. Linear regulators, especially, low dropout regulators which do not require any large passives, can be implemented digitally, are scalable across process nodes, and can potentially replace IVR or SCVR. A very fast simultaneous supply and clock modulation enabled with on-chip LDO and all-digital clock modulation (ADCM) circuit can facilitate increased randomization of side channel signatures to provide both point of load (PoL) regulation [40, 41] and security [53], therefore, simultaneously addressing the challenges of energy-efficiency and security for low-power IoT devices and high-performance computing systems.

1.1 Problem Statement

The objective of the proposed research is to explore energy-efficient and side channel attack resistant architectures for lightweight ciphers and design of generic low-overhead SCA countermeasures for cryptographic hardware by leveraging on-chip power management and clocking techniques. This includes:

- Development of energy-efficient and SCA resistant datapath architectures for 128-bit SIMON engine; which are subsequently characterized and quantified with respect to ASIC and FPGA implementations.
- Design of random fast voltage dithering (RFVD) scheme to enable side channel security for FIVRs which use on-package or bondwire based inductors.
- Characterization of power-supply glitch or temperature variation induced fault injection attack resistance offered by all-digital clock modulation (ADCM) circuit.
- Modeling and identification of different transformations induced by digital LDO which help in suppressing information leakage.
- Integration of hiding circuits into digital LDO control loop to improve SCA resistance.
- Characterization and quantification of power, EM and fault attack resistance through measurement from two prototype testchips.

1.2 Organization of this Thesis

Chapter 2 provides a brief background on several topics which are essential to comprehend the scope and contributions of this dissertation including lightweight cryptography, on-chip power management techniques, adaptive clocking, side channel attacks and countermeasures.

Chapter 3 describes side channel analysis methods and metrics employed in this dissertation to quantify SCA resistance. Also, presents the architecture for 128-bit AES (parallel AES: P-AES and serial AES: S-AES) and SIMON cores.

Chapter 4 explores different datapath architectures for SIMON for improved energy efficiency as well increased SCA resistance. Several datapath architectures utilizing bit-level and round-level parallelism are implemented on ASIC to investigate power, performance,

area (PPA) and energy tradeoffs. Proposed datapaths for 128-bit SIMON core are subsequently implemented on Sakura-G FPGA board to quantify side channel leakage. Optimized SIMON architectures are then applied to a low-power image sensor node to demonstrate the applicability and efficiency of the engine for IoT edge devices.

Chapter 5 presents lightweight countermeasures utilizing a FIVR and ADCM circuit to protect 128-bit AES cores against side channel attacks. The architecture of ADCM circuit is presented and various sources of randomization induced from ADCM including instantaneous frequency randomization (FR) in conjunction with FIVR loop randomization (LR) are discussed. SCA measurements from a testchip prototype consisting of FIVR, ADCM and AES cores designed and fabricated in 130nm CMOS process are presented and improvement in SCA resistance with respect to CPA & CEMA and TVLA analysis is discussed alongwith the limitations of the proposed countermeasures.

Chapter 6 explores fault injection attack (FIA) resistance offered by ADCM circuit for S-AES. A simple measurement setup is developed to inject power supply glitch and temperature variations based faults for the standalone S-AES and protected S-AES (with ADCM) systems. Faults are characterized and analyzed for FIA under different glitch settings and role of ADCM to tolerate these glitches is discussed and experimentally demonstrated.

Chapter 7 explores on-chip LDO regulators as countermeasures to side channel attacks for 128-bit AES and SIMON cores. Additional circuit techniques, namely switching noise injector (SNI) and random reference word generator (R-VREF), to randomize side channel signatures are described. Measurement results from a testchip consisting of all-digital LDO, SNI & R-VREF, AES and SIMON cores developed in 130nm CMOS process are presented and improvement in SCA resistance with respect to CPA & CEMA and TVLA analysis is discussed.

Chapter 8 highlights the contributions of this dissertation and discusses future research work and directions.

CHAPTER 2

BACKGROUND

2.1 Lightweight Cryptography

Even though IoT edge devices are miniscule and perform only important processing to reduce the communication from a device to the host machine, the processing of the data and communication need to be secured to prevent the edge device from becoming the entry point into the network for a potential hacker [Fig. 2.1]. Due to stringent resource requirements, conventional encryption schemes such as AES or DES cannot be used for IoT-edge nodes, giving rise to the field of lightweight cryptography . On one hand, researchers are exploring compact and low-power realization of AES engines, for example, using serial implementations [54–56], on the other hand, there is a growing interest in ultra-lightweight but cryptanalytically secure encryption algorithms that can be realized in very small area footprint and consume minimal energy. For example, lightweight cryptographic algorithms such as CLEFIA [32], PRESENT [31] and PRINCE [30] have been proposed and studied

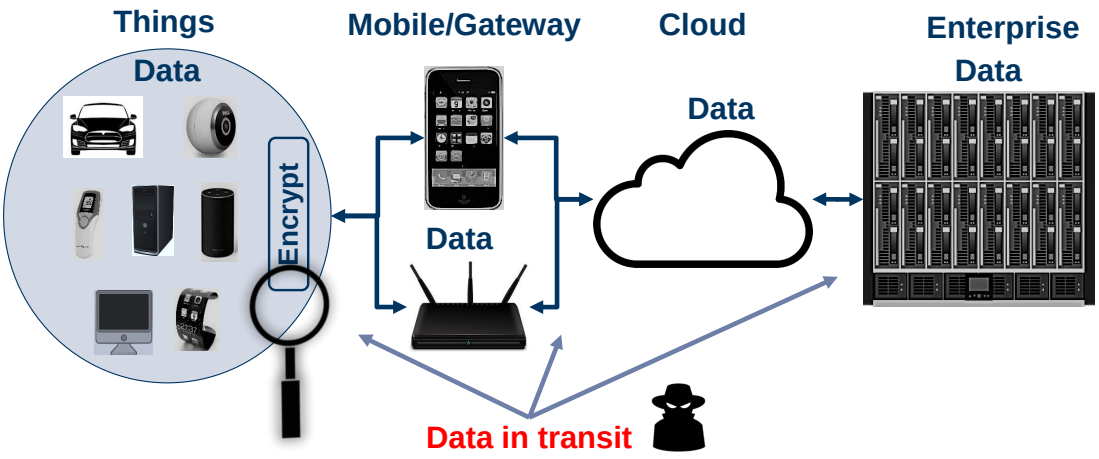


Figure 2.1: Security threats of the interconnected world where security (in terms of security protocols and defenses against physical attacks) must be the first priority and not optional.

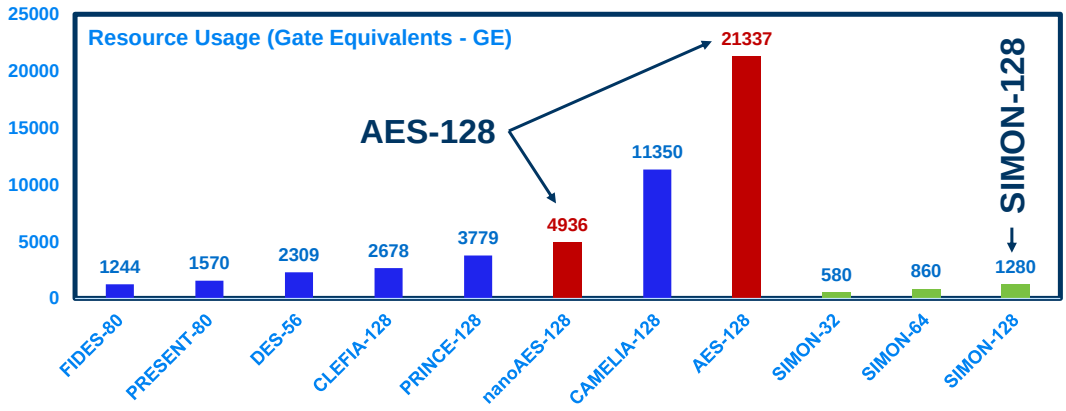


Figure 2.2: SIMON provides much higher flexibility when choosing an encryption algorithm for a target IoT application with respect to security parameters and with its resource-efficiency compared to other lightweight ciphers as well as compact implementations of AES algorithm.

for area, performance, and energy tradeoffs. More recently, National Institute of Standards and Technology (NIST) has proposed SIMON and SPECK [35], two sister lightweight cryptographic algorithms, tailored for IoT edge devices. SIMON is optimized for hardware implementations while SPECK is optimized for software implementations. The SIMON algorithm is based on feistel networks. Very simple round function and key expansion hardware makes SIMON suitable for lightweight cryptography. The high degree of algorithmic flexibility enables SIMON hardware to be optimized based on the application security requirement [Fig. 2.2].

Side channel attacks (SCA), a major threat to security of all cryptographic devices, have been shown to be very successful to extract the secret key. Many countermeasures which have been proposed to inhibit SCA in AES engines at significant area, power and/or performance overheads may not be suitable for lightweight cryptographic primitives. Moreover, there is an inherent tradeoff between compact implementation and SCA resistance of encryption engines. For example, serial implementation, a common approach for compact/low-power encryption engines, reduces algorithmic noise from parallel computation, thereby increasing SCA vulnerability. The bit-serial nature can reduce the SCA resistance of lightweight encryption algorithms even further. Consequently, there is a need to charac-

terize the tradeoff between area, performance, energy/power and side-channel security of encryption engines. While such analysis has been performed for AES engines, there is a lack of studies on how to design compact resource-efficient as well as SCA secure hardware engines for lightweight encryption algorithms like SIMON.

2.2 On-Chip Power Management

Computing systems have traditionally been optimized for performance driving technological innovations and shrinking the transistors to fit more and more devices on the same die for better integration and speeds. However, it was achieved at the cost of increased power consumption and resulting thermal and reliability concerns. To address these challenges, designs were optimized with respect to a power budget and at the same time several power management techniques were developed to reduce power consumption in order to improve system energy-efficiency. Among these techniques, dynamic power management (DPM) techniques such as dynamic voltage scaling (DVS) [37], dynamic votlage frequency scaling (DVFS) [38], power and clock gating [57, 58], multiple power domains are more popular. However, to fully utilize these techniques, voltage regulators (VRs) must be integrated on-chip to facilitate fine-grained and point of load regulation [39–41]. VRs are the basic building blocks of any low-power system and can be categorized into switching DC-DC converters and linear regulators [Fig. 2.3]. Switching DC-DC converters can further be divided into inductive or capacitive based on the passive used to store the energy during switching cycles while low-dropout (LDO) regulators are the most common implementations of linear regulators which are used for a low-power systems on chip (SoC). LDOs can be categorized into analog or digital LDOs based on the type of feedback loop (continuous or discrete). We employ inductive VR and digital LDO (DLDO) regulator in this research. These are briefly described below:

2.2.1 Fully Integrated Inductive Voltage Regulators (FIVR)

Modern processor systems switch between multiple power states quite frequently to save power under varying workload conditions. For off-chip VRs, parasitics of PCB and package PDN reduce the power conversion efficiency and limit the transient performance (settling time for load and reference transients). Therefore, to tackle these challenges, VRs are increasingly integrated on-chip to improve performance and energy-efficiency [39]. Relatively smaller parasitics (higher resonance frequency) for the on-chip PDN allows use of smaller passives for the FIVR increasing the power-density offered by these passives. Additionally, the control loop for the FIVR can be run at much faster speed. This not only improves the system performance but also drastically simplifies the integration of smaller passives [59] on the same chip. An all-digital implementation of the feedback controller can be chosen to simplify FIVR design [60–62].

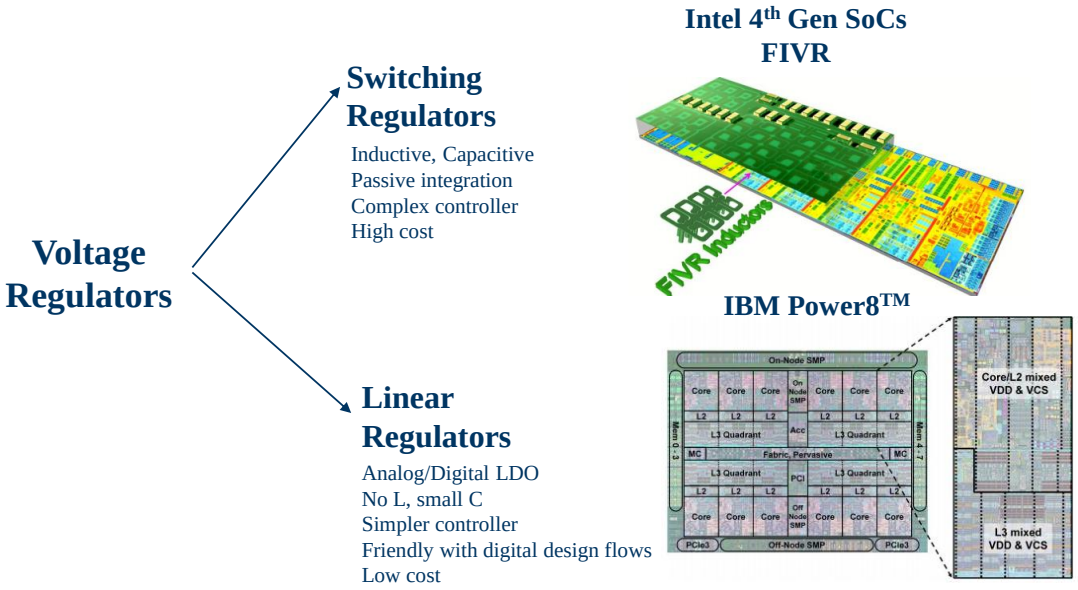


Figure 2.3: Categorization of different types of integrated voltage regulators used in modern power management systems.

2.2.2 All-Digital Low Dropout Regulators (DLDO

Even though FIVRs have smaller passives compared to their off-chip counterparts, they still consume significant on-chip resources. To eliminate the need for large passives, low dropout (LDO) regulators, especially digital LDO (DLDO) can be used. Compared to FIVRs, DLDOs do not require large passives, are simpler to design and are scalable across process nodes. Power losses for DLDOs are dominated by the power-stage losses which are determined by the dropout voltage across the power stage ($V_{IN,DLDO}$-V_{OUT}) where $V_{IN,DLDO}$ is the input supply voltage and V_{OUT} is the output voltage generated by DLDO. When the input supply voltage is fixed and output voltage is modified in accordance with DVFS power-stage transitions, the DLDO power conversion efficiency suffers at smaller output voltages. FIVRs can ideally provide 100% efficiency irrespective of output voltage. Therefore, for large systems, DLDOs are used alongwith FIVRs (FIVR followed by DLDO with DLDO closer to target load) for efficient power-management.

Digital low-dropout (DLDO) regulators can operate at very low supply voltages, can be digitally synthesized and are therefore preferred over their analog counterparts for their portability, scaling and ease of integration. Traditional digital LDOs utilizing shift-register (SR) based bang-bang control [63] are compact but suffer from poor transient performance. For improved transient performance, recent digital LDO architectures either have an additional loop (analog-assisted [64, 65] or employ proportional-integral (PI) or proportional-integral-derivative (PID) controller [41, 66–68]. For DLDOs with digital PID (DPID) controller in the feedback loop, the controller gains determine the open-loop system poles and zeros and are designed based on the desired stability (phase) margins and performance (bandwidth).

2.3 Adaptive Clocking

Modern processor systems run at greater than 1GHz clock frequency and draw current patterns which vary in less than 1 nanosecond resulting in nanosecond-speed droops in core supply voltage [43]. Traditionally, a supply guardband (or timing margin) has been added while characterizing the timing paths for a process, voltage and temperature (PVT) corner which leads to increased power consumption. To reduce the supply guardband (or timing margin), several techniques have been proposed [43, 69–72] and can be categorized into 1) timing error detection and prevention 2) adaptive clocking. The timing error detection and prevention circuits, such as Razor [72] and Razor II [73] rely on a modified flip-flop (FF) design to detect errors and correct them inside the FF (Razor) or via an architectural replay (Razor II). These circuits achieve energy reduction by lowering the supply voltage to the point of first failure (PoFF) and by purposely operating below PoFF since timing failures are very rare ($\sim$1 error in 10 million cycles) [73]. Another approach to manage timing failures under voltage or PVT fluctuations is to adapt the clock to ensure sufficient timing margin is available. To achieve that, several adaptive clocking techniques have been developed which employ distributed critical path monitors (CPMs) [69] or replicas (CPRs) [42] to measure critical path delay under the effect of noise and localized supply droops. These CPMs can either direct the central clock source (voltage-controlled-oscillator - VCO or phase-locked-loop - PLL) to update the clock in presence of a voltage droop or clock edges can be modulated locally. The response time for clock adaptation can be significant if the central clock source is involved in the clock adaptation due to feedback loop delay from the target CPM to the PLL. However, with local clock modulators, this feedback loop delay can be avoided. Compared to Razor or Razor II techniques, adaptive clocking can lead to smaller area overhead as FF design doesn't need to be modified. In modern processor systems, including central processing units (CPUs) from Intel, IBM and AMD, due to severity of workload, PVT and on-chip variations, some sort of adaptive clocking or

timing error detection or prevention is commonly employed to tolerate local supply droops and noise events.

2.4 Side Channel Attack and Countermeasures

Timing based side channel was the first one discovered by Kocher et. al. [4] in 1996 where he demonstrated that by carefully measuring the time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman (DH) exponents, factor RSA keys and break other cryptosystems. These attacks only require known ciphertext and can be conducted in a computationally inexpensive manner. Several preventing measures must be taken, such as constant-time implementations of these protocols, to thwart these attacks. Since 1996, several other side channels have been discovered including power based side channel by Kocher et. al. [12], EM side channel by Agrawal et. al. [5], fault based side channel by Boneh et. al. [74] etc. These attacks and several countermeasures developed to protect against these are described briefly here:

2.4.1 Power & EM based Side Channels and Countermeasures

In 1999, Kocher et. al. [12] proposed differential power analysis (DPA) to exploit the side channel leakage via power consumption of a data encryption standard (DES) cryptosystem to reveal the secret key used for encrypting the messages. Since then researchers have improved statistical analysis techniques. In 2004, Brier et. al. [13] proposed correlation power analysis (CPA) with a leakage model. In CPA, measured power is correlated with a hypothetical power model [using hamming distance between current state (target) and previous state of the circuit or hamming weight of the current state (target) of the circuit]. CPA improves the side channel analysis further. For extremely noisy or misaligned measurements, the frequency domain correlation frequency analysis (CFA) was proposed in [75]. Rohatagi et. al. proposed template attacks [14] to improve side channel analysis for encryption engines with countermeasures. Template attacks are carried out in 2-phases: 1)

profiling phase: measurements are captured from a device which is similar to target device for large number of plaintexts and known keys, the leakages are subsequently profiled based on a side channel distinguisher (similar to CPA power model) and 2) attack or testing phase: measurements from the target device are used to reveal the secret key by utilizing the templates created in the profiling phase. Recently, several advanced attacks using machine learning as well as deep learning techniques have been presented which improve the effectiveness of side channel attacks further while facilitating successful attacks on devices even with proven countermeasures.

In 2002, Agarwal et. al. [5] demonstrated side channel analysis techniques, simple EM analysis (SEMA) and differential EM analysis (DEMA), exploiting side channel leakage through EM emanations from a software implementation of DES algorithm on a smartcard. They showed that EM emanations can be used when power signatures are unavailable (or difficult to acquire) and for some cases even when some countermeasures are present to protect against power analysis attacks. The paper highlighted a key aspect of the nature of the EM side channel leakage, i.e., presence of multiple, unintentional, information-carrying signals.

Since side channel analysis using CPA or DPA is difficult in presence of countermeasures or noise, national institute of standards and technology (NIST) brought forth a test-vector leakage assessment methodology [76] to quantify side channel leakage from a protected device which can be used to validate effectiveness of proposed SCA countermeasures.

After power analysis attacks (PAA) were first introduced in [12], researchers have studied and proposed several countermeasures. All these countermeasures are based on two basic approaches: 1) information hiding and 2) information masking [77]. Hiding aims to either decrease the signal-to-noise ratio (SNR) or equalize the current drawn, making it independent of processed data. Masking relies on randomization of processing of key dependent intermediate data during the encryption. These countermeasures can further be

Table 2.1: Area and Performance overhead comparison for some of the popular countermeasures at different levels of hardware design.

Countermeasure	Type	Platform	Area	Performance	SCA Resistance	Year
Random Order Execution [15]	**Arch./ Algorithm**	**ASIC**	**15k**	**N/A**	**21×**	**2012**
Multiprocessor [16]		**Simulation**	**2×**	**0.4%**	**N/A**	**2008**
Masking [79]		**FPGA**	**3-4×**	**40-160×**	**N/A**	**2010**
Masking of SBOX [80]		**8051 MC**	**2.5-3×**	**40-60%**	**240×**	**2011**
PDDL/WDDL [18, 20]	**Logic**	**ASIC**	**2.3×**	**N/A**	**>24×**	**2006**
BCDL [24]		**FPGA**	**4×**	**2×**	**>20×**	**2010**
iMDPL [19]		**ASIC**	**18-19×**	**70%**	**>100×**	**2007**
Charge Recovery Logic [29]		**ASIC**	**3×**	**0%**	**720×**	**2015**
Noise Injection via PDN [78]	**Physical**	**Simulation**	**1.4×**	**0%**	**>13×**	**2014**
Current Equalizer [21]		**ASIC**	**1.25×**	**50%**	**>2500×**	**2009**
Clock Randomization [22]		**FPGA**	**1.1×**	**N/A**	**>30×**	**2011**

categorized at the architecture, logic or physical design level. Architectural countermeasures target random order execution [15] of instructions, insertion of NOPs (no operations) and dual core processor where bitflipped data is processed on another processor, thus equalizing the power [16]. Authors in [17] have proposed random order isomorphism which uses randomization for composite field arithmetic in Galois Field (GF). Most of the logic level techniques are based on differential dynamic logic (DDL) style and are dependent on equalization of current consumption. However, these techniques (PDDL [18], WDDL [20], MDPL, and iMDPL [19]) have huge area overheads and are not suitable for resource-constrained devices. Physical level techniques are based on noise injection [78], current equalization through switched capacitor [21] and clock randomization [22]. Noise injection needs additional noise generation circuitry, incurs power and performance overheads (not reported in [78]). Clock randomization provides limited improvement to MTD and researchers have developed higher order signal processing techniques to overcome the trace misalignment issue introduced by random clock edges. In summary, most of these schemes either have high area/performance overhead or do not provide adequate security. Table 2.1 summarizes some of the existing countermeasures and their area and power overheads. The overheads are compared with the base design (design without any countermeasure).

On-chip Power Management based SCA Countermeasures

The role of integrated voltage regulators in power attack has been studied in literature. SCA countermeasures based on on-chip integrated VRs can be built on top of the underlying encryption engines without requiring any modification to the design or implementation of encryption engine itself. Additionally, these SCA countermeasures are independent of the cryptographic algorithms so can be treated as generic countermeasures. Another major advantage with theses countermeasures is that they can be combined with existing architecture, logic or physical design based countermeasures to further improve the SCA resistance of encryption hardware.

Due to these advantages, there has been significant interest in exploiting on-chip voltage regulators and power-management techniques to enhance resistance to power and EM based SCA attacks. Telandro et. al. have shown that an LDO along with a switched capacitor converter can hide information in the load current; however, no actual attack study was performed [47]. Authors in [48] have proposed random converter gating of multi-phase switched capacitor converter (SCC) to provide security. However, area cost is huge for multi-phase SCC. In [49], authors have shown that fully integrated inductive voltage regulator (FIVR) can reduce the correlation between input and load currents. Based on correlation studies, it is shown that input current is poorly correlated to load currents in time domain; however, no power attack study was performed. Moreover, FIVR, although very promising for mobile SOCs, can significantly increase the overheads for lightweight encryption engines due to manufacturing complexity associated with an on-chip inductor. Das et. al. [81] presented a shunt LDO to attenuate AES current consumption and with simulations demonstrated improved power side channel analysis (P-SCA) attack resistance with noise injection on attenuated signature. Uzun et. al. [48] proposed converter-gating based on multi-stage SCC where interleaved stages are turned on/off in random fashion to scramble the power signature by introducing a timing uncertainty. Yang et. al. [44] presented measured results to show that randomized dynamic voltage frequency scaling

Table 2.2: Comparison of side channel analysis attack resistance offered by power management and low power techniques.

Power Management/Low Power Technique	Complexity	Area	PAA resistance analysis
Switched Cap. (SC) VR + analog-LDO	High	Moderate	Protection using SC-VR. No power attack analysis.
Random converter gating in multi-phase SCVR	High	High	Improvement in power trace entropy, no statistical power analysis
Fully Integrated Inductive VR	High	High	Power attack protection from control loop randomization
Integrated LDO	Moderate	Low	PAA protection with integration effects and feedback loop losses
Random Dynamic Voltage Frequency Scaling (RDVFS)	High	High	Max. N× increase in MTD where N number of V-F pairs
Dynamic Voltage Switching (DVS)	Moderate	High	Broken with instantaneous frequency analysis

(RDVFS) can help in designing SCA resistant cryptosystem.

Table 2.2 summarizes existing countermeasures that are based on power-management or low-power techniques. Both FIVR/SCVR based countermeasures are highly complex and require large area. RDVFS based countermeasures provide limited improvement in SCA resistance [N$\times$ where N is the number of voltage-frequency (V-F) pairs employed in the RDVFS based countermeasure]. DVS based SCA countermeasures have been shown to be broken with instantaneous frequency analysis [82] and do not offer much SCA resistance. This dissertation will propose circuit techniques and architecture to improve RDVFS countermeasures which provide much higher SCA resistance.

Compared to other SCA countermeasures, integrated LDO based SCA countermeasures have relatively moderate design complexity and require smaller area and therefore are very attractive. However, the existing research work that utilizes integrated analog and digital LDO is limited and is mostly based on simulation studies [81, 83–86]. This dissertation investigates all-digital LDO as an SCA countermeasure and develops circuit techniques to improve SCA resistance for different encryption engines.

2.4.2 Fault based Side Channels and Countermeasures

Fault Injection Attacks (FIA)

Fault injection attacks (FIA) are another form of side channel attacks [74, 87–89] and can be conducted inexpensively in a non-invasive manner. FIA relies on injection of a precisely timed/located fault during the cryptographic operation. Differential fault analysis (DFA) is subsequently performed between correct and faulty output to reveal secret information. Several fault injection techniques, such as variations in power supply, irregularities in clock input, X-ray or electromagnetic (EM) emissions, temperature variations and directed laser beams [90–92] can be employed to deliberately modify an integrated circuits (IC) operating conditions to alter its computation. FIA based on supply, clock or temperature modification is low cost and easier to implement, therefore is highly practical. However, in most cases, clock is not accessible to an adversary, therefore clock glitch-based FIA cannot be conducted. Supply glitches, on the other hand, are easier to generate externally which then propagate to chip internal circuits resulting in timing failures.

Software/hardware level countermeasures are incorporated to detect and correct faults as well as to increase tolerance to FIA to ensure data privacy/integrity [27, 93–97]. In 1996, Boneh et. al. demonstrated fault attacks for the first time to extract cryptographic keys from public-key cryptosystem (RSA) [74]. Subsequently, fault-based attack models were applied to several block ciphers (DES [87], AES [88]). Several works have presented fault models ranging from 1-bit to single-/multi- byte [88, 89]. 1-bit faults are difficult to induce; therefore, byte faults are preferred. Additionally, fault models which require less number of faulty outputs are desired. Several works have shown supply/clock glitch-based FIA on FPGA or smartcards [92]. Existing works on clock/supply glitch-based fault attacks assume that glitches can be injected in a precise manner assuming an adversary has complete knowledge of the underlying cryptographic hardware in terms of exactly when round operations are computed. However, in absence of such knowledge, it is very difficult

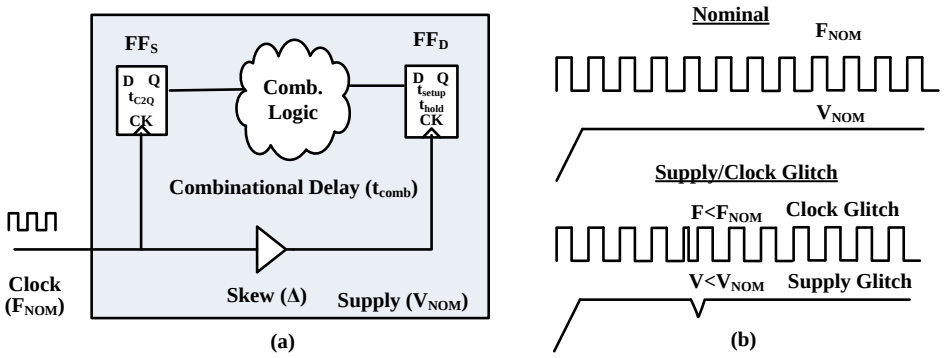


Figure 2.4: (a) Timing properties of a digital circuit depend on supply and clock and (b) may fail when supply/clock based glitch is injected.

to inject faults at the desired locations. Authors of [90] demonstrated FIA for AES on a cryptographic LSI, however, the clock was generated externally using FPGA with precise control on the clock edges. Authors of [91] demonstrated an FIA on ARM-based android device. Underpowering, overclocking and temperature variations-based FIA relies on timing failures in the digital circuits. Under modified operating conditions, data may either arrive too late at a flipflop (FF) or too early leading to setup (Eq. 2.1) or hold (Eq. 2.2) failure, respectively [95, 96] [Fig. 2.4]. Any fault mitigation technique attempts to detect these timing errors, masks the faulty output (under FIA) and performs the operation again.

$$t_{c2q,max} + t_{comb,max} + t_{setup} \leq t_{ck} + \Delta_{ck,min} \tag{2.1}$$

$$t_{c2q,min} + t_{comb,min} \geq t_{hold} + \Delta_{ck,max} \tag{2.2}$$

Countermeasures against Fault Injection Attacks (FIA)

There have been several countermeasures proposed to prevent FIA. Countermeasures can be categorized in - 1) detection and correction [93], and 2) infection: propagating difference in intermediate states to multiple bytes of the ciphertext making it unexploitable [94]. Since the primary mechanism for the fault injection is timing failures, error-resilient architectures such as duplicated complemented datapath [27], tunable replicas [95, 96], glitch

detector circuit [97], synchronous Razor [72] family can be used to detect and correct errors in presence of supply glitches. Additionally, instead of stalling the pipeline for an erroneous operation, the instantaneous clock frequency can be adapted in a pre-emptive manner to prevent the timing failures [43]. However, major drawback with most of the adaptive circuits is their complexity and slow response time. To prevent any fault propagating outside, the adaptive circuit must respond at cycle-by-cycle speed and for an easier integration with the current digital design flows, it must be fully synthesizable.

CHAPTER 3

SIDE CHANNEL LEAKAGE CHARACTERIZATION

3.1 Measurement Methodology

The measurement methodology used in this dissertation is briefly described here. More details will be provided during the subsequent chapters, wherever required.

3.1.1 Measurement of Power Signatures

For both FPGA and ASIC platforms, the power signatures are acquired across a 1Ω resistor on board. Single ended measurements are acquired at the resistor node closer to the ASIC/FPGA prototype under the assumption that due to large decoupling capacitors, the other node of the resistor has only very low frequency signals. SMA cables terminated with 1MΩ equivalent impedance are used to probe the targeted node. Tektronix oscilloscope (DPO5204) is used to capture the power signatures at sampling speed of 1Gbps and bandwidth of upto 500MHz. An internal trigger (for FPGA) and an external trigger (for ASIC) are used to trigger the oscilloscope. The data from scope buffer is read via a USB cable or over Ethernet. All the postprocessing is performed using Python based analysis platform.

3.1.2 Measurement of EM Signatures

For capturing EM signatures, passive EMC probes from Beehive electronics are used [98]. These probes have an electrostatic shield integrated in the probe loops to eliminate common mode pickup. Two different probes used in the experiments are described below:

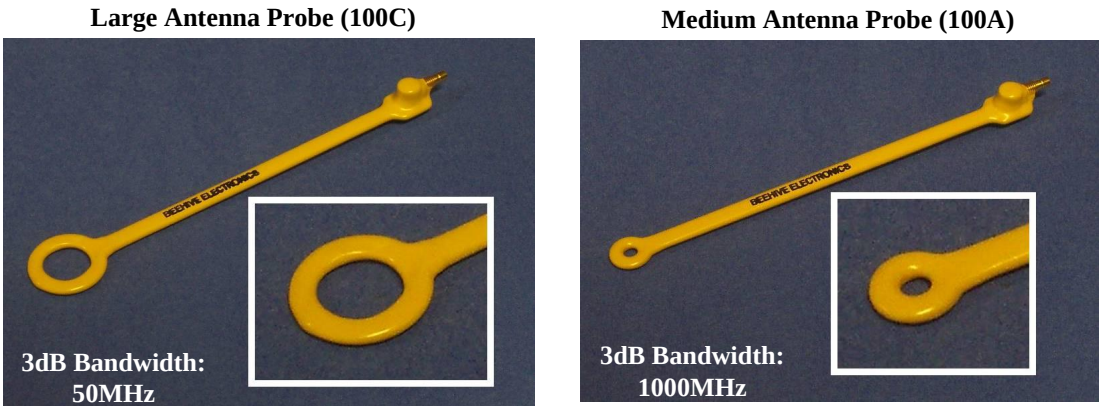


Figure 3.1: Two different EMC probes from Beehive Electronics [98] with different loop area are used in our experiments.

Large Antenna Probe - 100C

The large antenna probe has tip diameter of 1.0" and loop diameter of 0.85". It has a 3dB frequency of 50MHz and first resonance frequency of 500MHz. Due to larger area, it has very high sensitivity to EM emissions but is limited in terms of capturing high frequency signatures and spatial resolution.

Medium Antenna Probe - 100A

The medium antenna probe has tip diameter of 0.5" and loop diameter of 0.4". It has a 3dB frequency of 1000MHz and first resonance frequency of 2600MHz. With smaller loop, this probe can accurately capture high frequency signatures and provides very fine spatial resolution. However, it is limited in terms of probe sensitivity as this probe has to be kept in close proximity of the EM source.

These probes are connected to SMA cables to interface with the oscilloscope, with 1MΩ termination at the oscilloscope side, similar to that for power side channel measurement. The probe locations have been optimized based on targeted location of the testchip for attack. Also, probe type (large or medium loop) was chosen considering localized or globalized EM probing requirements.

3.2 Statistical Methods

3.2.1 Signal to Noise Ratio (SNR)

The side channel leakage can be modeled in terms of signal to noise ratio. It is defined as below for measured power/EM traces:

$$L(x) = \epsilon \times |\phi(x)| + L_0 + N(0, \sigma^2) \tag{3.1}$$

where ϵ is the leakage conveyed by the one-bit toggle and is the signal, $\phi(x)$ is the leakage model related to the plaintext and the key, noted x, L_0 is average circuit power due to activity of other parts of the design, $N(0, \sigma^2)$ is an additive white Gaussian noise (AWGN). Signal (ϵ) can be modeled as covariance between measured traces and leakage model which is given by:

$$\epsilon = \frac{cov(L, M)}{4n} \tag{3.2}$$

where M is leakage model based on hamming distance (HD) or hamming weight (HW) and n is the number of bits in the intermediate variable. The SNR with this leakage model is given as [99]:

$$SNR = \epsilon / \sigma \tag{3.3}$$

3.2.2 Correlation Power/EM Analysis (CPA/CEMA)

CPA is performed between the measured power consumption and a hypothetical model to reveal the correct key [13]. Hypothetical models aim to model the current drawn by the encryption hardware during the encryption and are generally based on hamming distance (HD) between 2 intermediate variables or hamming weight (HW) of an intermediate vari-

able. CPA is based on Pearson's correlation defined as below:

$$\rho_{t,k} = \frac{\sum_{i=1}^{N}[(s_{t,i} - \overline{s_t})(h_{k,i} - \overline{h_k})]}{\sqrt{\sum_{i=1}^{N}(s_{t,i} - \overline{s_t})^2 \sum_{i=1}^{N}(h_{k,i} - \overline{h_k})^2}} \tag{3.4}$$

where $\rho_{t,k}$ is pearson's correlation coefficient for time instant *t* and key guess *k*. $s_{t,i}$ is the signal value for time instant *t* and trace *i*. Similarly, $h_{k,i}$ is the hypothetical model for key guess *k* and trace *i*. After pearson's correlation is computed for all key guesses $k \in K$ where K is the set of all key hypothesis and time instants $t \in T$ where T is the number of time samples, a correlation trace ρ_k is obtained for each k and plotted against time. The correct key hypothesis k_c will have the highest correlation out of all $|K|$ hypotheses as described below:

$$k_c = \underset{k}{\operatorname{argmax}}(|\rho_{t,k}|) \tag{3.5}$$

A minimum-traces-to-disclose (MTD) metric is defined as number of measurements required to reveal k_c. We define two other metrics to quantify the success of the CPA attack - 1) success rate (SR) and 2) correlation ratio (CR).

Success Rate (SR)

SR is defined as below:

$$SR = \frac{\sum_{d=1}^{D} R(sk_d)}{D} \times 100(\%) \tag{3.6}$$

where D is the number of subkeys, sk_d is the d^{th} subkey and $R(sk_d)$=1 if sk_d is correctly revealed, 0 otherwise. For our AES cores, each byte is a subkey (D=128/8=16) while for SIMON core, each nibble is a subkey (D=128/4=32). Proposed circuit techniques are compared wrt MTD required for 80% SR, i.e., to reveal 80% of all the subkeys (13/16 for AES cores, 25/32 for SIMON core).

Correlation Ratio (CR)

CR is defined as below:

$$CR = \frac{max(\rho_{k_c})}{max(\rho_k)} \ , \ k \in K \setminus k_c \tag{3.7}$$

where ρ_{k_c} is the correlation trace for correct key guess k_c while ρ_k is the correlation trace for key guess k. $CR > 1$ indicates successful attack. For P-AES, 8-bit HD based hypothetical model is derived between the ciphertext and the output of 9th round while for S-AES, 8-bit HW based hypothetical model is derived at the output of SBOX operation in the 1st round [100]. For SIMON, 1-bit HD based model between two consecutive bits is used at output of 2nd round [101]. Each intermediate variable chosen for both AES cores has 8-bit key dependency ($|K|$=2^8=256) while for SIMON the key dependency is 4-bit ($|K|$=2^4=16). CPA is also performed in the frequency domain which helps in reducing the effect of signal misalignment [75]. CEMA follows the same steps but is performed on EM signatures instead of power signatures [5].

3.2.3 Test Vector Leakage Assessment (TVLA)

TVLA is a standard statistical hypothesis testing methodology to validate SCA resistance offered by a countermeasure. Leakage from intermediate variables of any sensitive algorithm are detected using TVLA where the collected traces are divided into two sets (*A* and *B*) with null hypothesis that these sets have statistically indistinguishable mean and variance [76]. The alternate hypothesis being different mean and variance. A Weltch's t-test is performed on the two sets and a t-statistic of >4.5 indicates leakage with 99.9999%.

$$t - statistic = \frac{\mu_A - \mu_B}{\sqrt{\frac{\sigma_A^2}{N_A} + \frac{\sigma_B^2}{N_B}}} \tag{3.8}$$

where μ_A and μ_B are the means of, σ_A and σ_B are standard deviations of and N_A, N_B

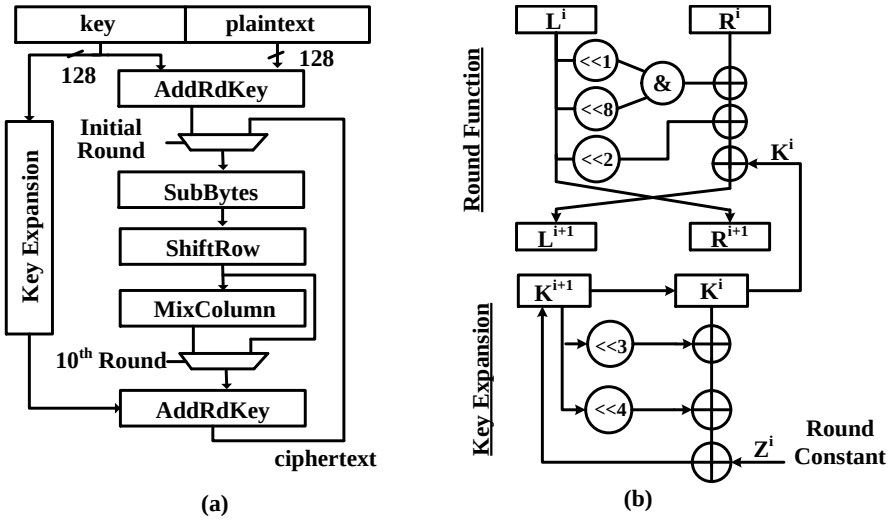


Figure 3.2: Cryptographic algorithms employed in this paper to evaluate improvement in SCA resistance: (a) 128-bit AES algorithm and (b) 128-bit SIMON algorithm.

are number of traces in sets A and B. All the computations are performed point-wise for each time sample.

3.3 Architecture of Encryption Engines

This section presents datapath architecture for hardware implementations of 128-bit AES and SIMON algorithms [Fig. 3.2] implemented in ASIC as well as FPGA platforms to investigate the impact of proposed countermeasures in the subsequent chapters.

3.3.1 Architecture of 128-bit AES Engines

Advanced Encryption Standard (AES) algorithm is the de-facto encryption algorithm used in modern communication systems to encrypt messages (plaintext) using a secret (key) to generate encrypted messages (ciphertext). It supports block size of 128 bits and key sizes of 128, 192, 256 bits based on the security requirements. AES algorithm is based on substitution-permutation-network (SPN) and has complex round functions with 10, 12, 14 rounds of operations based on the key size. There is also an initial round which just performs AddRoundKey (key XOR'ing with the input message). Along with AddRoundKey, SubstituteBytes (SBOX), ShiftRow (SR), MixColumn (MC) are the other round operations

[Fig. 3.2(a)]. Depending on the target application, the hardware for AES algorithm can be optimized in several ways. We have implemented two different datapaths for AES- 1) Parallel AES (P-AES) with 128-bit parallel datapath [Fig. 3.3(a)] [102] and 2) Serial AES (S-AES) [54] with 8-bit serial datapath [Fig. 3.3(b)]. All the round operations are implemented in hardware using finite-field arithmetic. For both P-AES and S-AES, the same round hardware is re-used (round-reuse) for computing all the rounds. SBOX is the most expensive operation of AES algorithm, therefore for S-AES, only 1 SBOX is implement to compute 1-byte at a time and the same is shared for key expansion hardware. For P-AES, all the bytes of the intermediate state are computed in parallel while for S-AES, each byte of the intermediate state is computed serially. P-AES takes 11 cycles to compute 1 encryption including initial round while S-AES has 502 cycles encryption latency. In our implementations, P-AES can only perform encryption while S-AES, due to its unified datapath, can perform both encryption and decryption [Fig. 3.3(b)].

3.3.2 Architecture of 128-bit SIMON Engine

SIMON is based on Fiestel Networks (FN) with very simple round function. Confusion and diffusion properties are achieved using large number of rounds for SIMON compared to AES which has complex round function. SIMON provides high level of flexibility in terms of block size (32-bit to 128-bit) and key size (64-bit to 256-bit) to enable efficient selection of parameters based on target application and required security specifications. Considering stringent area and power requirements, we have implemented bit-serial (the most compact) datapath for 128-bit SIMON [Fig. 3.4] [103]. There are 68 rounds of operation with each round consisting of 1-AND and 3-XOR 2-input operations . The bit-serial datapath computes 1-bit in 1-cycle with 64-bits processed in each round. The total encryption latency is 4352 (64$\times$68) cycles. Both encryption datapath and key expansion datapath is implemented using shift registers divided into left word (L^i) and right word (R^i). L^i is further divided into 56-bit shift register and two 8-bit shift registers to manage

the control flow. A round-counter and a bit-counter is used to generate the mux select signals for selecting the bits from the upper byte (DU^j) or the lower byte (DL^j). Compared to both AES engines, SIMON engine has significantly smaller area but has much worse performance and energy consumption due to long encryption latency [101].

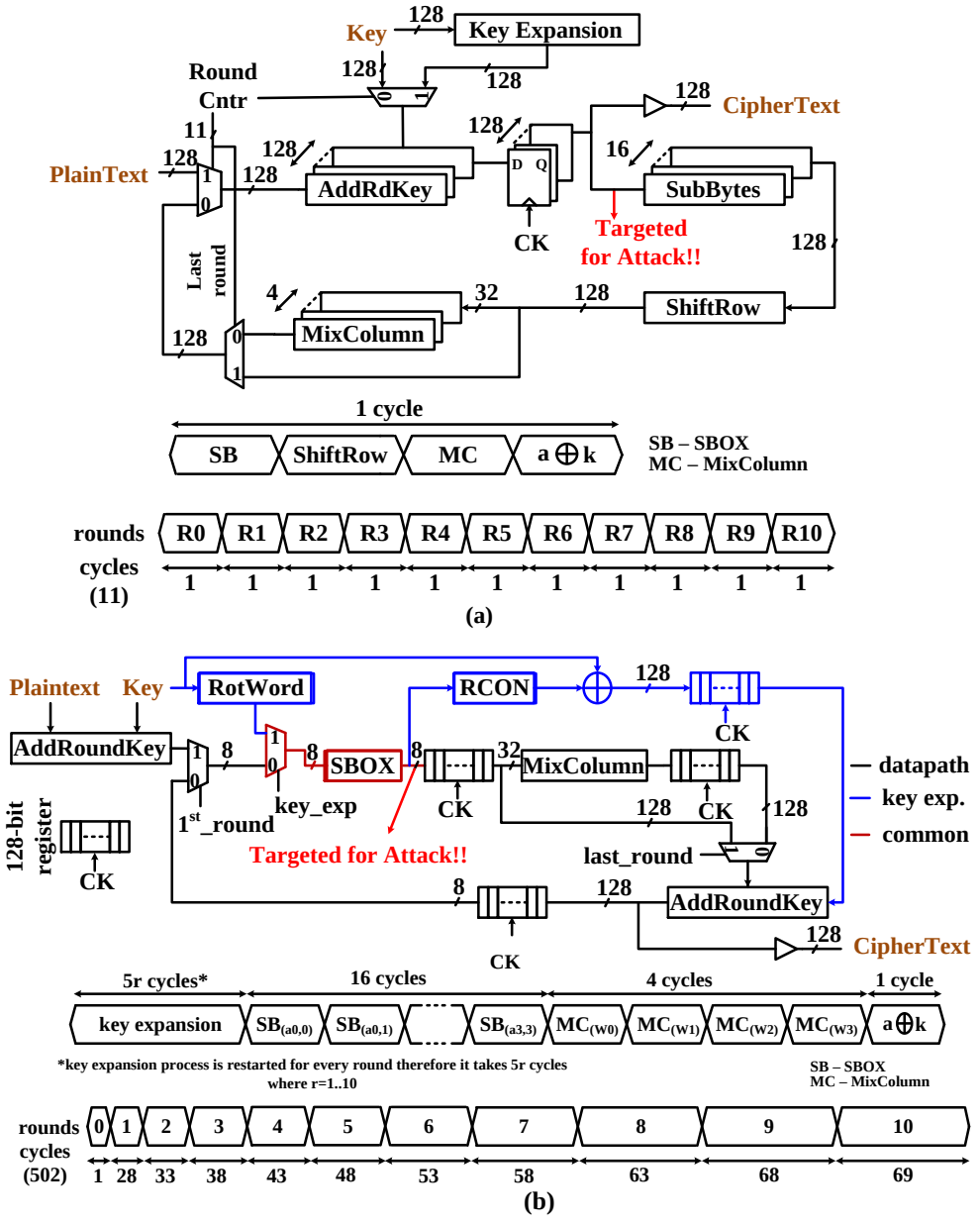


Figure 3.3: Datapath architectures for 128-bit (a) P-AES and (b) S-AES encryption cores.

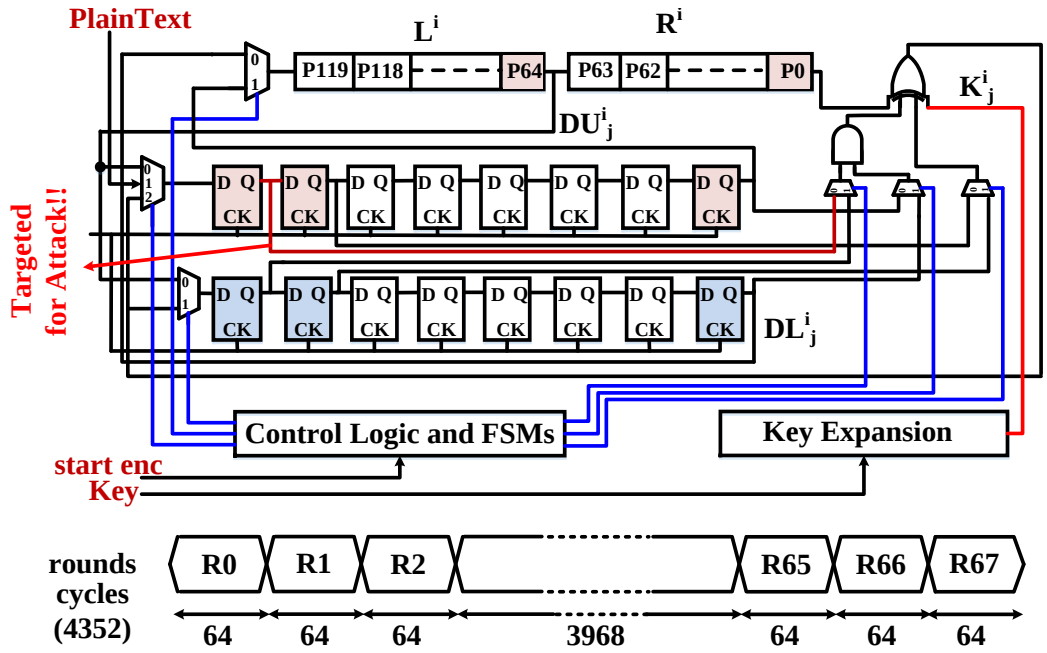


Figure 3.4: Datapath architecture for 128-bit SIMON encryption core.

3.3.3 Threat Model

Throughout this thesis, there have been several assumptions that have been made about the attack scenarios. These assumptions are described below:

- An adversary can gain physical access to the device, perform encryption/decryption operations using his own plaintexts/ciphertexts and can measure power and EM signatures. For power measurements, it is assumed that the adversary can put any resistor on the power-supply path to measure voltage drop across the resistor.

- Local supply node of encryption engines, which is exposed outside through a pad for experiments in this work only, will not be accessible to an adversary for a commercial system unless specifically mentioned in the subsequent chapters.

- Neither Pseudo-random seed nor the structure of the circuits used to randomize power/EM signatures is known to the adversary so they cannot find the exact patterns of the output of these randomized circuits. Even though some of these circuits are programmed externally for characterization/validation/flexibility purposes, on a

commercial product, after characterization, the desired settings should be written on write-only registers without external access.

- Note that an adversary can perform some statistical analysis on the measured power/EM signatures to reveal the random pattern which is possible but non-trivial and is outside the scope of this work.

- Power measurements are only performed at the supply node, not the ground node. However, EM measurements capture signatures from both supply and ground nodes and on-package/on-chip power-delivery network as well as signal interconnects.

- This work assumes first order CPA attacks and all the improvement in SCA resistance results are based on first order CPA attacks only. Higher order attacks, such as template attacks (TA), mutual information analysis (MIA), moment correlating DPA (MC-DPA), machine/deep learning (ML/DL) attacks may/may not provide better attack results but are outside the scope of this work.

CHAPTER 4
ENERGY-EFFICIENT AND SCA-RESISTANT LIGHTWEIGHT CRYPTOGRAPHY

With the rise of miniscule devices in the form of internet of things (IoTs), internet of everything (IoEs) [2], security has become a major concern not only for these devices but also for the entire network these devices connect to as the network is as secure as its least secure device. Therefore, there is a need for integrating security features even in the devices which perform minor tasks and may not be critical with respect to security. Considering the stringent resource requirements for IoT devices, SIMON lightweight cryptographic algorithm, developed by National Security Agency (NSA) and standardized by NIST [35], seems to be a viable option as it offers flexible levels of security. Based on the security requirements of the target application, the design of SIMON block cipher can be modified at the algorithm level (such as block size, key size, etc) and at the architecture level (bit-level and round-level parallelism) to meet the resource requirements as depicted in Fig. 4.1.

There have been several lightweight cryptographic primitives proposed recently to satisfy the need to secure resource constrained devices. These consist of block and stream ciphers as well as hash functions [30–35, 104, 105]. Some recently proposed lightweight schemes such as CLEFIA [32, 106], CAMELLIA [107], PRESENT [31], PRINCE [30], SIMON and SPECK [35, 108], can be implemented with very small area and power using serial datapaths. However, these serial architectures lag in performance and do not essentially provide energy optimal operation. Moreover, serial architectures are highly susceptible to power side channel analysis (P-SCA) attacks because of no algorithmic noise from parallel computation. Recently, some attention has been given to optimizing lightweight ciphers with respect to energy consumption as well as performance. Authors in [109] have presented a lightweight cipher named Midori which was optimized for energy using round

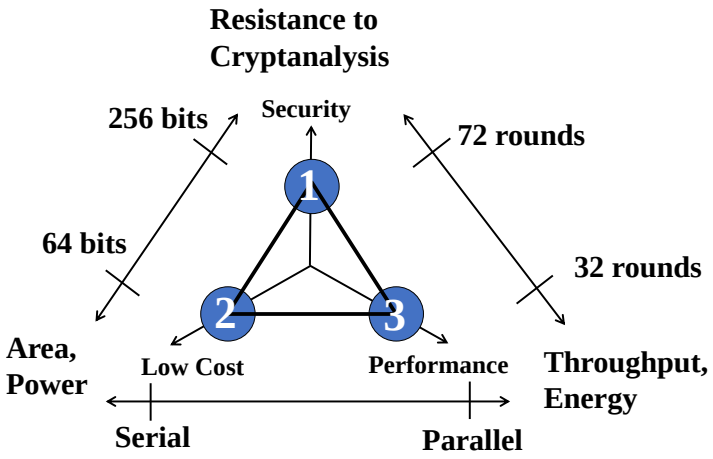


Figure 4.1: Available algorithmic/architectural design space for SIMON enabling flexible tunable security for based on application requirements.

unrolling techniques. Similarly, authors in [110–112] have explored energy efficiency for several lightweight cipher schemes. With a model for energy consumption, it was shown that energy consumption has quadratic relationship with degree of unrolling. Conventionally, different datapath architectures have been explored for AES to optimize for area [54, 55, 102] but very few works have focused on optimizing for energy efficiency [56].

Most of the countermeasures that exist today, either designed with architectural modifications or different logic styles to mask or hide information [83] have huge area, power and/or performance overheads. In-spite of their effectiveness, these countermeasures cannot be implemented for lightweight cryptographic ciphers due to limited resources. Moreover, serial architectures of these lightweight ciphers, in absence of any algorithmic noise, tend to have increased side channel leakage. Therefore, it is extremely critical to develop countermeasures which can be easily integrated with these schemes with very low resource requirement [83–85].

Different datapath architectures for lightweight ciphers [113, 114], specifically for SIMON algorithm [Fig. 3.2(b)] have already been studied for smaller footprint or higher performance [36, 115, 116]. Authors in [36] implement a bit-level serial architecture for very small area targeted for IoT edge devices, however, the design suffers from very poor

energy efficiency due to long encryption latency. Authors in [115] design reconfigurable datapath for SIMON on FPGA (Spartan-6) for varying block and key sizes. Similarly, [116] proposes a round-level pipelining (breaking round function in multiple pipeline stages) to improve the throughput at the cost of increased latency and area. Moreover, bitserial architectures for SIMON have already been explored for the side channel leakage in [30, 31], however, the impact of other datapath architectures on side channel leakage has not been previously explored. In [117], authors show that bitserial architecture for SIMON 64/96 can be protected against Correlation Power Analysis (CPA) attacks with masking at 66.6%, and 13.4% cost to area and performance respectively. Similarly, authors in [118] perform differential power attack (DPA) on serial implementations of 32b and 64b SIMON on FPGA with a hypothesis complexity of 176. However, none of the prior works focus on finding power, performance and area (PPA) tradeoffs. Moreover, an architecture optimized for power may not necessarily provide optimal energy consumption, specifically for serial implementations which take higher number of cycles to compute the ciphertext. In this chapter, we focus on optimizing datapaths for 128-bit SIMON (SIMON128) for energy consumption and subsequently quantify the side channel leakage for different datapath architectures. We then analyze the application of the optimized datapath on an image-sensor node and compute the overheads for side-channel secure communication.

This chapter explores the design space for SIMON datapath considering tradeoffs between area, performance, power, energy and P-SCA resistance. In particular, we have investigated the role of round unrolling for SIMON with respect to energy consumption, performance and P-SCA resistance [Fig. 4.2]. The chapter builds on several prior works in the design of lightweight cryptographic algorithms and makes the following key contributions with respect to design space exploration for 128-bit SIMON (SIMON128):

- We have explored and optimized serial and parallel datapath architectures including round unrolling for SIMON128 with respect to power, performance, area and energy for ASIC (15nm) and FPGA (Spartan-6, 45nm) implementations.

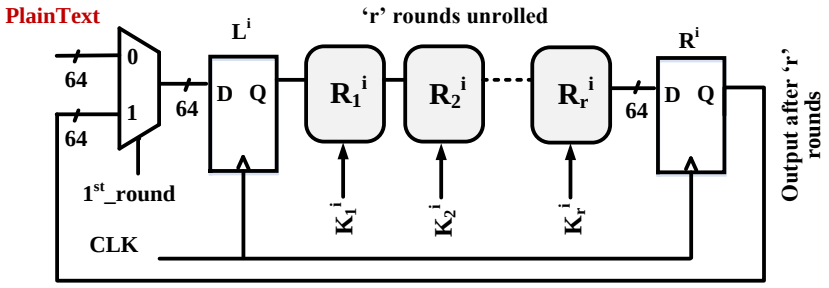


Figure 4.2: Unrolled architectures for lightweight cryptographic algorithms provide optimal energy at very high performance while simultaneously improving resistance against power side channel analysis attacks.

- We have measured side channel leakage for various SIMON datapath architectures (using FPGA) and quantified minimum-traces-to-disclosure (MTD) required for a successful Correlation Power Analysis (CPA) attack and signal-to-noise ratio (SNR).
- We demonstrate that round unrolling can significantly enhance the side-channel security through deep diffusion of the input key when sufficient rounds are unrolled.
- We have compared the energy-efficiency and power attack resistance of presented SIMON designs with high-performance (parallel) and compact (serial) AES designs.
- We have applied the optimized SIMON encryption engine into a low-power image sensor node to demonstrate the applicability and efficiency of the engine for IoT edge devices.

The rest of the chapter is organized as below. Section 4.1 presents alternative datapath architectures (ASIC and FPGA) for 128b SIMON (SIMON128); Section 4.2 presents the side-channel measurement results; Section 4.3 presents optimized datapath for enhanced P-SCA resistance; Section 4.4 presents the application of encryption engines to an image sensor node and overhead analysis; and Section 4.5 summarizes the key findings.

4.1 Energy-Efficient Hardware Architectures for SIMON-128

Hardware implementations of SIMON128 can be realized at different levels of parallelism starting from a bit serial to fully parallel. The design choice for different datapath architectures leads to power, performance and area (PPA) tradeoffs. Bit-level parallelism can be exploited with 1-bit to 64-bit parallel datapaths for SIMON128. Beyond bit-level, parallelism can be exploited at round-level with up to 68 rounds unrolled [Fig. 4.2]. Our work explores the tradeoffs in area, power, throughput and energy for these different architectures of SIMON128.

4.1.1 ASIC Implementations of SIMON128 Block Cipher

For ASIC implementations, different architectures are synthesized using CMOS 15nm NanGate FreePDK15 open cell library and power, performance, area and energy consumption values are subsequently computed.

1-bit Serial (Bitserial) Datapath

The bitserial implementation takes 64 cycles per round for 68 rounds [3.4] [119]. It consists of 64-bit shift register (L^i and R^i) to store the intermediate states of round operation. There is only one computational unit comprising of 2-input AND and 4-input XOR gate (or 3 2-input XOR gates). Two 8-bit shift registers (DU^i and DL^i) are required due to circular shift pattern of the round function. These registers alternate in storing the values computed after each round. Most Significant Byte (MSB) of plaintext is stored in DU^i at the start of encryption. The output of 8-bit shift registers (DU^i and DL^i) is connected to Li through a 2:1 MUX which uses branch select derived from bit-counter and round-counter control logic. For even rounds, L^i is connected to DU^i during first 8 cycles and to DL^i during remaining 56 cycles. For odd rounds, these connections are reversed. Similarly, output of computational unit (next state L^{i+1}) is connected to DL^i for even rounds and to DU^i for

Algorithm 1: Pseudocode for Bitserial SIMON.

L: Left (upper) word, **R**: Right (lower) word, **K**: Key
DU: Shift register Upper, **DL**: Shift register Lower
DU^i: Plaintext (MSB), nRounds: number of rounds
for $i \leftarrow$ *0 to nRounds* **do**
  for $j \leftarrow$ *0 to 64* **do**
    if *i mod 2* **then**
      if *j* < 8 **then**
        $L^i \leftarrow DU^i$
      else
        $L^i \leftarrow DL^i$
      end
      $L_j^{i+1} \leftarrow F(DU^i(8), DU^i(2), DU^i(1), R^i(0), K^i(0))$
      $DL^i \leftarrow L_j^{i+1}$
    else
      if *j* < 8 **then**
        $L^i \leftarrow DL^i$
      else
        $L^i \leftarrow DU^i$
      end
      $L_j^{i+1} \leftarrow F(DL^i(8), DL^i(2), DL^i(1), R^i(0), K^i(0))$
      $DU^i \leftarrow L_j^{i+1}$
    end
  end
end

odd rounds. AND is computed using 1-bit shifted and 8-bit shifted values of (L^i) and it is XORed with 2-bit shifted value of (L^i), lower plaintext bit (R^i), input key bit (K_j^i). The bit generated is loaded into shift register (DU^i or DL^i) based on round counter and bit counter which in turn is loaded into L^i. The ciphertext obtained at the end of 68th round is stored in state registers L^i and R^i. bitserial datapath is described in algorithmic steps below [Algorithm 1]. The area utilization for bitserial architecture is minimum, however, encryption throughput is also very small.

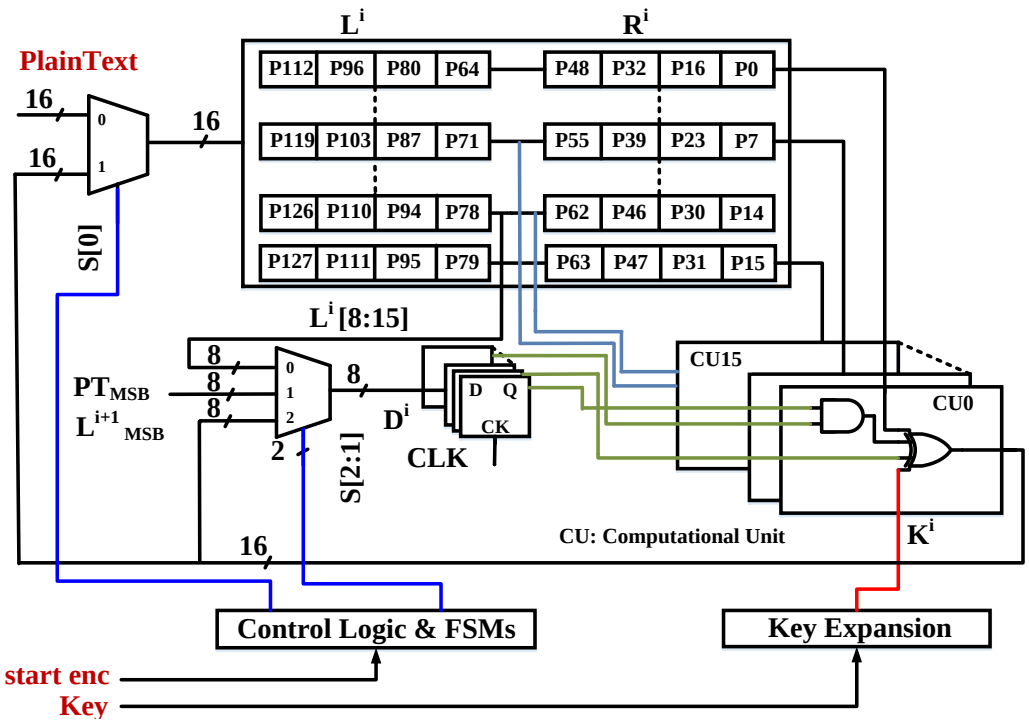


Figure 4.3: 16-bit parallel datapath architecture for SIMON128.

16-bit Parallel Datapath

16-bit parallel datapath has 16 parallel shift registers, each storing 4-bit data. The implementation takes 4 cycles per round and up to 68 rounds for entire encryption. The state after plaintext is loaded is shown in Fig. 4.3. The computational units have increased from 1-AND / XOR to 16-AND / XOR gates. There is 8-bit parallel register (D^i) that stores most significant byte of plaintext while loading plaintext, 2nd byte of L^i after every cycle and most significant byte of the 16-bit output of the computational unit at the end of every round (new state L^{i+1}). The loading of corresponding value in D^i is controlled with 3:1 MUX with select signal generated based on bit-counter and round counter values. The inputs to 16 parallel computational units are derived from D^i, L^i and R^i. 16-bit parallel datapath is described in steps in Algorithm 2. Compared to bitserial datapath, 16-bit parallel implementation occupies more area due to higher number of computational units (no/very small change in register area) and results in improved throughput by a factor of 4×.

Algorithm 2: Pseudocode for 16-bit Parallel SIMON.

DW: Datapath Width = 16
L: Left (upper) word, **R**: Right (lower) word, **K**: Key
D: 8-bit parallel register
if *load_plaintext* **then**
  for $i \leftarrow$ *0 to 7* **do**
    $plaintext \leftarrow data[i * DW : (i+1) * DW]$
    $D_i \leftarrow plaintext[MSB]$
  end
else if *run_encryption* **then**
  for $i \leftarrow$ *0 to nRounds* **do**
    for $j \leftarrow$ *0 to (64/DW)* **do**
      $L_0^{i+1} \leftarrow F(L^i(63), L^i(62), L^i(55), R^i(0), K^i(0))$
      $L_1^{i+1} \leftarrow F(L^i(0), L^i(63), L^i(56), R^i(1), K^i(1))$
      $L_0^{i+1} \leftarrow F(L^i(1), L^i(0), L^i(57), R^i(2), K^i(2))$
      .
      .
      .
      $L_{15}^{i+1} \leftarrow F(L^i(14), L^i(13), L^i(6), R^i(15), K^i(15))$
      $D_i \leftarrow L^i[8:15]$
    end
    $D_i \leftarrow L^{i+1}[MSB]$
  end
  else
    DONE!
  end

64-bit Parallel Datapath

64-bit datapath has 128-bit register to store the plaintext and intermediate data (L^i and R^i) during computation of rounds [Fig. 4.4]. There are 64 computational units each consisting of AND and XOR gates. The inputs to the computational units are bits stored in Li and Ri. The critical path delay for 64-bit architecture is smaller compared to bitserial architecture due to less complex control structure (bitserial processes 1-bit at a time based on bit-counter control logic). The encryption takes 68 cycles (1-cycle per round) and improves the latency by a factor of 64$\times$ with respect to bitserial architecture, therefore improving the energy efficiency and performance significantly. The steps (pseudocode) for 64-bit datapath are given in the Algorithm 3.

Algorithm 3: Pseudocode for 64-bit Parallel SIMON128.

L: Left (upper) word, **R**: Right (lower) word, **K**: Key

for $i \leftarrow$ *0 to nRounds* **do**

$L_0^{i+1} \leftarrow F(L^i(63), L^i(62), L^i(55), R^i(0), K^i(0))$

$L_1^{i+1} \leftarrow F(L^i(0), L^i(63), L^i(56), R^i(1), K^i(1))$

$L_0^{i+1} \leftarrow F(L^i(1), L^i(0), L^i(57), R^i(2), K^i(2))$

.

.

.

$L_{63}^{i+1} \leftarrow F(L^i(62), L^i(61), L^i(54), R^i(63), K^i(63))$

$D_i \leftarrow L^i$

$R^{i+1} \leftarrow L^i$

end

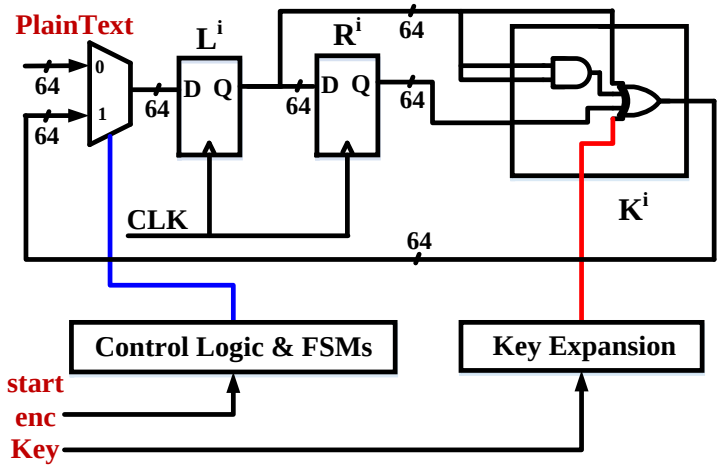


Figure 4.4: 64-bit parallel datapath for SIMON.

Round Unrolled Datapaths

To further improve the energy efficiency and performance, round unrolled datapath architectures were implemented with varying degree of round unrolling (2-round to 6-round unrolling). Round unrolled architectures implement multiple rounds in single cycle. Latency is determined based on the number of rounds unrolled. A 3-round unrolled architecture is depicted in Fig. 4.5. 3 round operations, each logical replica of 64-bit computational unit, are computed in a single cycle. The inputs to these round functions are intermediate states L^i and R^i as well as expanded keys K^i. The output generated from each round function is used as inputs to next round. Therefore, intermediate sequential state obtained

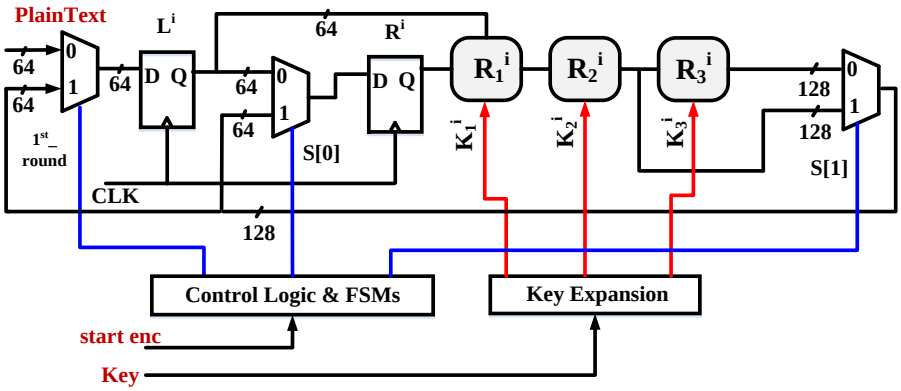


Figure 4.5: 3-round unrolled datapath architecture for SIMON128. It is the most energy optimal implementation with respect to ASIC implementations of all dapapaths for SIMON128.

after each cycle is the output state after 3 rounds of computation. For 3-round unrolled design, number of rounds is not a multiple of degree of unrolling. So, last cycle has to unroll only twice to ensure correct operation. This is achieved using a 2:1 bypass mux at the output, which selects between 3-round and 2-round unrolled output based on a cycle counter. Round unrolling leads to better optimization of datapaths as synthesis tool (Synopsys Design Compiler - DC) merges the computation units and optimizes them together. Therefore, when we increase the degree of unrolling from 1 to 2, there is very small impact on the maximum achievable frequency (from 16.9GHz to 12.6GHz, 25.5% reduction, Table 4.1). In a complex algorithm such as AES and DES, round unrolling will approximately double the critical path delay, therefore halving the achievable clock frequency. This is the primary reason that benefits of round unrolling are only observed for lightweight ciphers which have very simplistic round functions [110].

When degree of round unrolling is further increased, the benefits reduce and after r=4, there is no benefit of unrolling the rounds with respect to energy consumption and performance. Also, area is now linearly proportional to degree of unrolling [Table 4.1]. The trend in power, performance and energy for different hardware implementations are shown in Fig. 4.6. An increasing trend in the area depicts the increased utilization of hardware resources for parallel architectures. As shown in Fig. 4.6(a), sequential elements do not

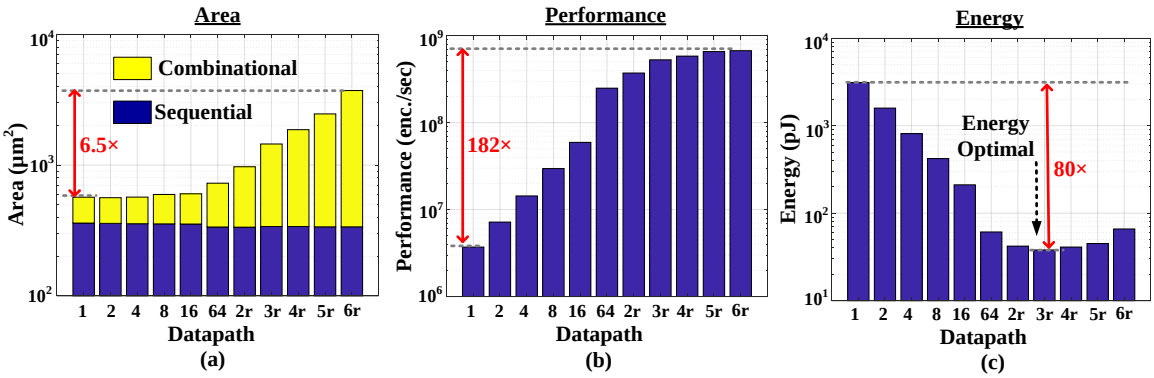


Figure 4.6: Design tradeoffs for different hardware architectures for SIMON128 with respect to ASIC implementations, (a) area, (b) performance and (c) energy. 3-round unrolled datapath gives the optimal energy while offering very good performance.

Table 4.1: Comparing area, performance, power and energy consumption for bitserial, parallel and round unrolled datapath architectures for SIMON128 from designs synthesized in NanGate FreePDK15 technology.

Datapath	Area (μm²)		Perf.		Power (mW)	Energy (pJ/enc.)
	Reg.	Comb.	Freq. (GHz)	Latency (cycles)		
1b	360	208	16	4352	11.5	3113
4b	356	213	15.6	1088	11.7	812
8b	355	241	16.1	544	12.5	421
16b	354	249	16.1	272	12.6	211
64b	336	391	16.9	68	15.4	61.7
64b, 2r	335	636	12.6	34	15.7	42.1
64b, 3r	339	1111	11.6	23	20.6	38.9
64b, 4r	339	1527	10	17	24.2	41.6
64b, 6r	337	3380	7.4	12	44.5	72

change much across different architectures, but combinational area increases with datapath width and degree of unrolling due to bit-level and round-level parallelism requiring more computational units. A sharp increase is observed in performance for bit-level parallel architectures followed by very small increase with unrolling for smaller degree r. Throughput (encryptions/second) is a function of max achievable frequency (critical path delay) and total latency (fixed for a particular datapath architecture [Fig. 4.6(b)]. Latency is reduced with parallel architectures which results in improved performance but with unrolling, multiple rounds are processed in each clock cycle reducing the total latency by a factor of r. For

Table 4.2: Comparison of SIMON128 architectures from this work with state-of-the-art lightweight ciphers and traditional AES128 architectures implemented on ASIC.

	Key Size	Block Size	Cycles / Block	Throughput @100KHz (Kbps)	Logic Process	Area (GE)
PRESENT-80 [31]	80	64	32	200	180nm	1570
CLEFIA-128 [106]	128	128	176	73	130nm	2678
Camellia [107]	128	128	20	640	350nm	11350
PRINCE [30]	128	128	1	533.3	45nm	3779
FIDES-80 [113]	80	64	47	10.64	45nm	1244
SPECK [108]	128	64	1	100	130nm	16371
SIMON [108]	128	64	1	100	130nm	23584
DES [112]	56	64	144	44.4	180nm	2309
AES128 [102]	128	128	11	1163	110nm	21337
nano AES128 [54]	128	128	336	38.1	22nm	4936
This work: SIMON						
Datapath	**Key Size**	**Block Size**	**Cycles / Block**	**Throughput @100KHz (Kbps)**	**Logic Process**	**Area (GE)**
1b	128	128	4352	2.9	15nm	2889
64b	128	128	68	188	15nm	3698
64b, 3r	128	128	23	582	15nm	7375
64b, 6r	128	128	12	1067	15nm	18905

smaller r, the reduction in latency dominates the increase in critical path delay and therefore, the energy consumption decreases initially. Fig. 4.6(c) shows that energy optimum is achieved for r=3 for ASIC implementations. For battery powered IoT edge devices, total energy consumption is an important parameter and energy consumption should be decreased per operation for a longer battery life.

Table 4.2 compares our SIMON128 datapath architectures with other state-of-the-art lightweight ciphers as well as AES block cipher. For technology independent comparison, gate equivalent count is compared for area and throughput is computed with respect to 100kHz design clock (all designs should easily meet this frequency). We observe that since most of the block ciphers have complex substitution operation in each round, the hardware cost is high and/or encryption throughput is poor. Also, as opposed to SIMON, these algorithms due to algorithmic as well as hardware complexity, cannot be efficiently unrolled to obtain higher energy efficiency. Of all the ciphers reported, AES in [102] has an equivalent performance at similar resource requirement (AES128 vs SIMON128, 64b, 6 round unrolled datapath). Therefore, an end-user can choose between AES128 and SIMON128 based on the side channel security they offer without any additional countermeasure. In the

next sections, FPGA implementation and measurement setup for side channel analysis will be presented and discussed for various datapath architectures of SIMON128 and compared against AES datapaths.

4.1.2 FPGA Implementations

RTL generated for different architectures are synthesized and mapped into Sakura-G based Xilinx Spartan-6 FPGA chip to observe the PPA trend. The board has an interface for reliable exchange of data between Main and Control FPGA chips [Fig. 4.7(b)]. The plaintext is sent from PC through a USB interface. A state machine is designed to load the plaintext and key into registers, execute the cipher operation and to generate the trigger signal when ciphertext is generated. After mapping, optimizations were done to ensure highest frequency operation for these designs. Voltage difference across a 1 resister on the FPGA board gives the current consumption during the encryption and energy numbers per encryption are subsequently computed based on current drawn during encryption. Table 4.3 shows that FPGA implementations also have similar trend as ASIC with reduced energy consumption for parallel datapaths and minimum energy consumption was obtained for 6-round unrolled design. We should note that 6-round unrolled datapath for SIMON128 can achieve better energy efficiency compared to AES128 (1.85× better than 128b datapath and 65.2× better than 8b datapath for AES128) while offering at-par (128b datapath for

Table 4.3: Comparing area, performance, power and energy consumption for bitserial, parallel and round unrolled datapath architectures for SIMON128 from designs programmed on Sakura-G FPGA (Spartan 6, 45nm process).

Algorithm	Data-path	Area		Perf.		Energy (nJ/enc.)
		Reg. (slices)	Logic (slices)	Freq. (MHz)	Latency (cycles)	
SIMON128	1b	499	525	250	4352	423
	64b	480	757	294	68	6.5
	64b, 3r	481	804	223	23	1.68
	64b, 6r	481	1692	145	12	0.46
AES128	128b	1000	3302	167	11	0.852
	8b	1030	1306	164	500	30

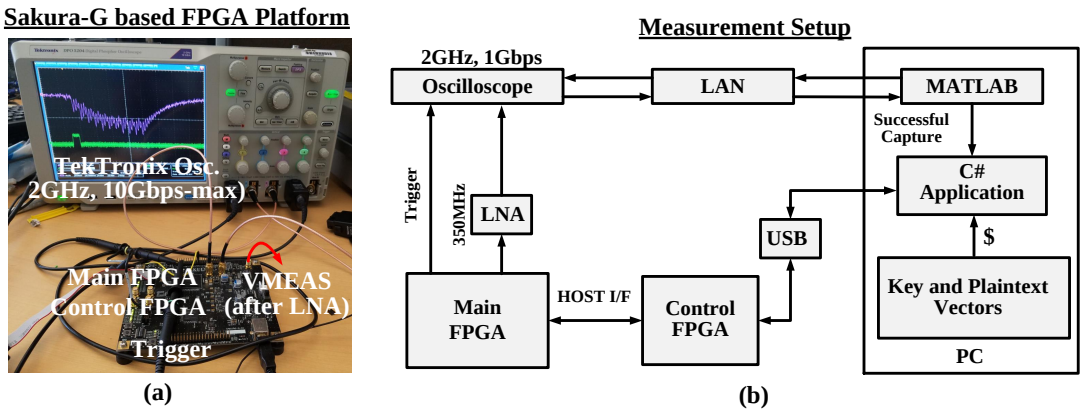


Figure 4.7: (a) Sakura-G based side channel leakage characterization platform and (b) measurement setup details.

AES128) or better (8b datapath for AES128) performance (encryption latency and throughput).

4.2 Side Channel Analysis of SIMON128 on Sakura-G

To quantify the side channel leakage characteristics of different hardware architectures of SIMON128, the current signatures were captured and then statistically analyzed to extract the secret key. In this section, we discuss the measurement setup and measured side channel characteristics for different SIMON128 architectures.

4.2.1 Measurement Setup

Side channel measurements were captured from Sakura-G based SCA leakage evaluation platform [Fig. 4.7(a)]. Randomly generated plaintext vectors and a fixed input key are loaded on to the main FPGA chip from PC using an USB interface and control FPGA chip [Fig. 4.7(b)]. Since current consumption from serialized SIMON128 implementations are expected to be small, an on-board LNA is utilized to amplify the signatures by $\sim$10$\times$. A trigger signal generated from main FPGA internally is used to trigger the Tektronix DPO5204 oscilloscope (2GHz bandwidth) which captures the targeted part of the power signatures at 1Gbps sampling rate.

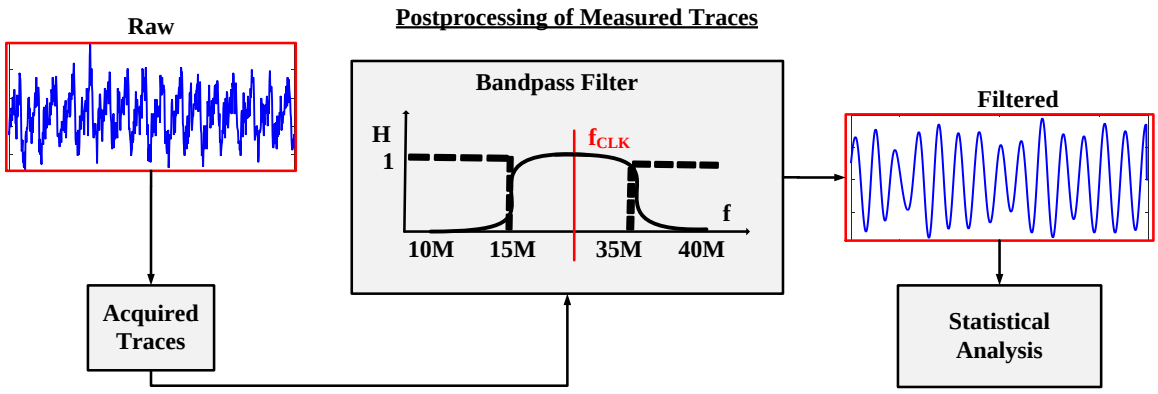


Figure 4.8: Postprocessing of measured power traces with band pass filter to remove out-of-band noise.

4.2.2 Postprocessing of Side Channel Traces

Raw signatures captured from oscilloscope have significant out-of-band noise. The success of any side channel analysis method depends on the signal-to-noise ratio for the captured signatures. To remove out-of-band noise, the captured traces are filtered using band pass filter (15MHz to 35MHz) centered at SIMON128 design clock frequency (24MHz) as shown in Fig. 4.8. Statistical analysis is performed on these filtered traces. Fig. 4.9 and 4.10 show raw and filtered power traces for bitserial and 64-bit datapath architectures respectively. The instantaneous current consumption from a bitserial architecture is very small and therefore very small variations are observed in the captured power signatures. On the other hand, 64-bit datapath architecture consumes a lot of power during each clock cycle because of parallel computation of 64 bits, therefore, large variations are observed in the captured power signatures. In Fig. 4.10(a), one can easily identify the clock frequency and the rounds during encryptions.

4.2.3 Metrics for Side Channel Leakage Quantification

To quantify the side leakage from different datapath architectures for SIMON128, we performed two statistical analyses, 1) Signal-to-Noise Ratio (SNR) and 2) Correlation Power Analysis (CPA). Both methods are described in chapter 3.2.1 and chapter 3.2.2.

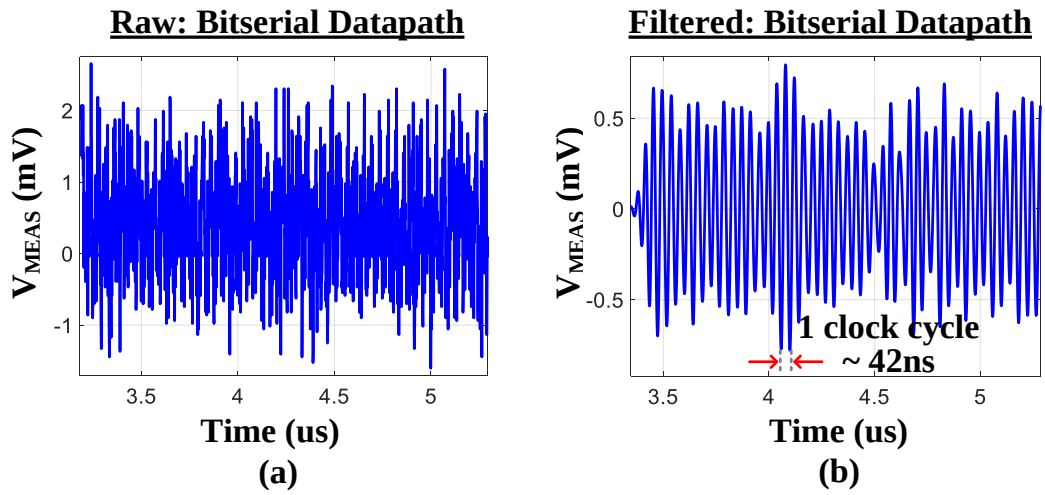


Figure 4.9: Measured power traces for bitserial datapath, (a) raw power trace, (b) filtered power trace.

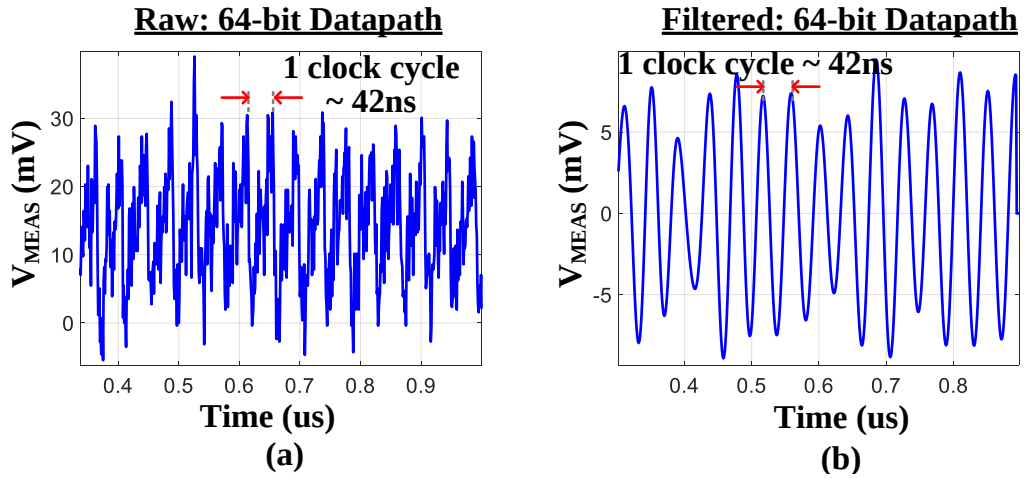


Figure 4.10: Measured power traces for 64-bit datapath architecture (a) raw power trace and (b) filtered power trace. Raw signatures show significant voltage variations during round operation for 64-bit datapath as all bits are computed in parallel.

4.2.4 Side Channel Attack on Bitserial SIMON128

Bitserial architecture for SIMON128 computes one bit at a time and then serially shifts this bit in the 8-bit registers. Fig. 4.11(a) shows two initial round functions. We target intermediate state after 2nd round (L^3) for CPA as it has dependencies on input keys K^1 and K^2 (no need for key expansion in first two rounds). Eq. 4.1 and Eq. 4.2 shows the dependency of LSB of L^3 ($L^3[0]$) on K^2 and L^2 which in turn are dependent on K^1. By tracing all the dependencies back to K^1 and K^2, we see that $L^3[0]$ is dependent on $K^2[0]$

through a single XOR gate and on $K^1[62]$ through 3 cascaded XOR gates. Fig. 4.11(b) shows all input key dependency paths (in total 4 paths 1, 2, 3 and 4) for $L^3[1:0]$. We understand that by flipping any bit of K^1 and K^2, the output bit dependent on K^1 and K^2 through XOR gates only will just be flipped irrespective of plaintext. Therefore, for a hamming weight or hamming distance power model, some key guesses will have same or inverted hypothetical values if we include these key dependencies, leading to same absolute correlation values for these key guesses. To negate same absolute correlation values, we ignored any key dependencies based on XOR gates only.

$$L^1 = plaintext[127:64], \quad R^1 = plaintext[63:0]$$

$$K^1 = key[63:0], \quad K^2 = key[127:64]$$

$$L^3[0] = (L^2[63] \& L^2[56]) \oplus L^2[62] \oplus K^2[0] \oplus R^2[0] \tag{4.1}$$

$$L^2[63] = (L^1[62] \& L^1[55]) \oplus L^1[61] \oplus K^1[63] \oplus R^1[63] \tag{4.2}$$

$$L^3[0] = f(K^2[0], \mathbf{K^1[56]}, K^1[62], \mathbf{K^1[63]}) \tag{4.3}$$

$$L^3[1] = f(K^2[1], \mathbf{K^1[57]}, K^1[63], \mathbf{K^1[0]}) \tag{4.4}$$

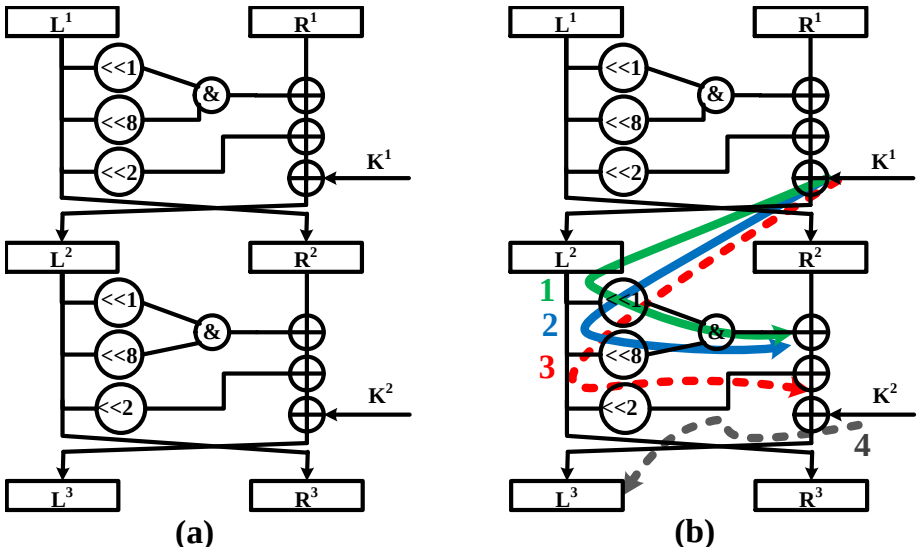


Figure 4.11: (a) Intermediate state after completion of 2 rounds, L^3, is targeted for attack and (b) key dependency paths for L^3.

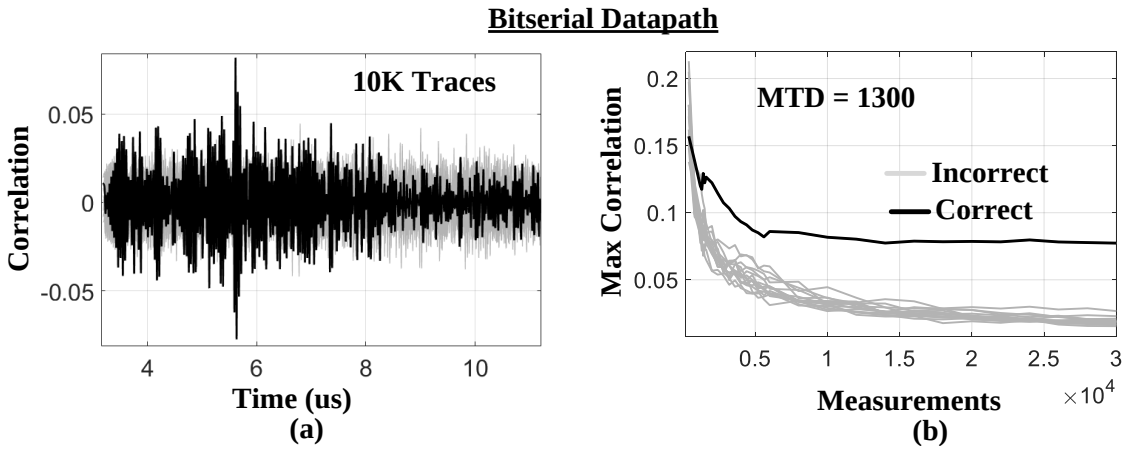


Figure 4.12: Successful attacks for bitserial datapath architecture: (a) correlation vs time plot shows successful attack with 10,000 measurements and (b) MTD vs number of measurements plot shows MTD of 1300.

Bits $L^3[0]$ and $L^3[1]$ are processed in consecutive cycles and computed bit is written on the same register. So, output of this register is a good candidate for switching activity dependent leakage through power consumption. Power model is derived by computing hamming distance between $L^3[0]$ and $L^3[1]$ and is dependent on bits 63, 57, 56, 0 of K^1 as highlighted in Eq. 4.3 and Eq. 4.4 and no bits of K^2 after ignoring XOR only dependencies. We make 16 guesses for these 4-bits (24) and CPA analysis on the measured power traces can disclose the correct key guess (0011) based on the highest correlation [Fig. 4.12(a)]. Since there is no algorithmic noise from any parallel computation, the SNR is high (0.163) which is also reflected in minimum-traces-to-disclosure (MTD) required to disclose the correct key with 1300 measurements only [Fig. 4.12(b)].

4.2.5 Side Channel Attack on Parallel SIMON128

Parallel datapath architectures can significantly improve performance (encryptions/second) and energy as demonstrated in previous sections. Moreover, since all the bits in a round are computed in parallel, the algorithmic noise contributed to computation of targeted bit in a CPA attack from computation of other bits is significant and therefore, the signal-to-noise ratio (SNR) is expected to degrade for parallel datapaths [Eq. 4.5] leading to increased

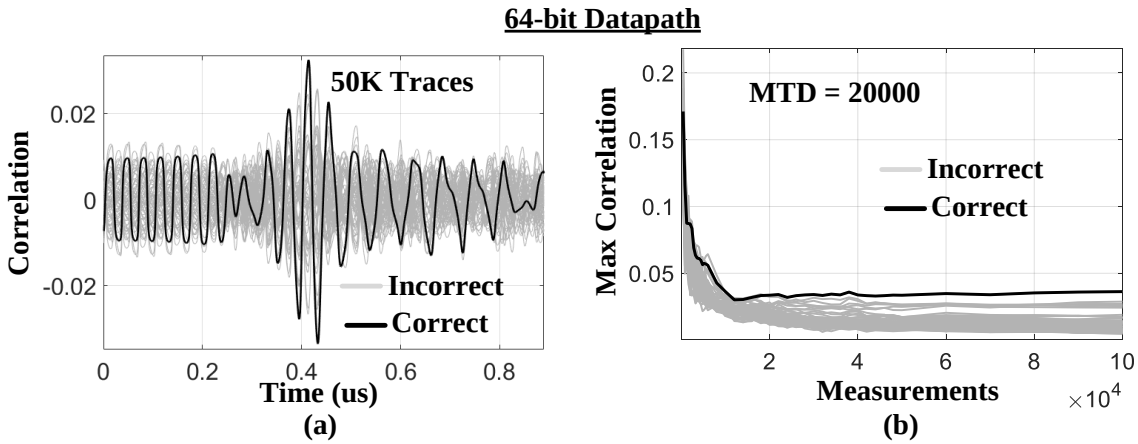


Figure 4.13: Successful attacks for 64-bit parallel datapath architecture: (a) correlation vs time plot shows successful attack with 10,000 measurements and (b) MTD vs number of measurements plot shows MTD of 20,000 indicating an improvement of 15× over bitserial datapath architecture.

difficulty or more measurements required for performing an SCA attack.

$$SNR = \frac{P_{analyzed\,bit}}{P_{parallel\,bits} + P_{other\,bits}} \tag{4.5}$$

We measured side channel characteristics for 16-bit and 64-bit datapath implementations of SIMON128 to analyze the impact of algorithmic noise. Fig. 4.13(a) shows the CPA attack performed on 3-bit hamming distance between $L^2[2:0]$ and $L^3[2:0]$. The useful key dependency is with respect to L^3 only as L^2 has XOR-only dependency on K^1. Eq. 4.6 to Eq. 4.9 list all the dependencies tracing back from L^3 to input plaintext and key while highlighting XOR-only key dependencies. Eq. 4.10 to Eq. 4.12 derive key dependencies for all the bits used for hamming distance computation while highlighting only useful key dependencies. Eq. 4.13 combines all key dependencies to compute 3-b hamming distance (useful key dependencies only). Please note that we could not mount a successful CPA with 1-bit and 2-bit hamming distance models demonstrating difficulty in recovering secret key for 64-bit datapath.

$$L^3[0] = (L^2[63] \& L^2[56]) \oplus L^2[62] \oplus \mathbf{K^2[0]} \oplus R^2[0] \tag{4.6}$$

$$L^3[1] = (L^2[0] \& L^2[57]) \oplus L^2[63] \oplus \mathbf{K^2[1]} \oplus R^2[1] \tag{4.7}$$

$$L^3[2] = (L^2[1] \& L^2[58]) \oplus L^2[0] \oplus \mathbf{K^2[2]} \oplus R^2[2] \tag{4.8}$$

$$L^2[63] = (L^1[62] \& L^1[55]) \oplus L^1[61] \oplus \mathbf{K^1[63]} \oplus R^1[63] \tag{4.9}$$

$$L^3[0] = f(K^2[0], \mathbf{K^1[56]}, K^1[62], \mathbf{K^1[63]}) \tag{4.10}$$

$$L^3[1] = f(K^2[1], \mathbf{K^1[57]}, K^1[63], \mathbf{K^1[0]}) \tag{4.11}$$

$$L^3[2] = f(K^2[2], \mathbf{K^1[58]}, K^1[0], \mathbf{K^1[1]}) \tag{4.12}$$

$$L^3[0] = f(K^1[63], K^1[58], K^1[57], K^1[56], K^1[1], K^1[0]) \tag{4.13}$$

The required MTD (5200) for 16-bit datapath was 4× more than bitserial design while for 64-bit datapath it was 20000, at least 15× more than bitserial [Fig. 4.13(b)]. Similarly, SNR decreases to 0.0419 indicating 3.9× degradation with respect to bitserial datapath. These results show that we can opportunistically exploit parallel datapath architectures to improve SCA resistance in addition to reduced energy and increased performance.

4.3 Improved SCA Resistance with Round Unrolling

Round unrolling has been previously proposed as a simple countermeasure for data encryption standard (DES) encryption scheme [120]. However, DES is not suitable for lightweight cryptography and unlike SIMON128, unrolling DES comes at a huge cost to area as well as power due to complexity of algorithm and its hardware implementation. With round unrolling, the keys are highly diffused in the datapath as well as during key expansion. Therefore, there must be a stronger hypothesis on multiple key bits (more number of guesses about the key) for a successful attack, making the attack infeasible with correlation power analysis if the degree of round unrolling is sufficiently high.

For a r round unrolled datapath, the noise characteristics is very much like 64b datapath, however, since r rounds are processed per clock cycle, the sequential elements are updated only after r rounds. It has been earlier demonstrated [121] that most of the side channel leakage comes from sequential elements in the encryption circuit as combinational logic have significant spurious switching generated due to difference in signal arrival times at digital gates. This not only leads to misalignment of points of interest but also reduces the SNR in the measured signatures. In this section, we demonstrate that with round unrolling, we can significantly improve the SCA resistance of SIMON128. Side channel leakage was measured for 3-round unrolled (3r) and 6-round unrolled (6r) datapaths. For 3r datapath, intermediate state L^4 was targeted at the end of 3rd round (as opposed to end of 2nd round for bitserial and parallel datapaths as sequential elements are only updated at the end of 3rd round in this case). All the computation steps to find useful key dependencies tracing back from $L^4[0]$ to input key and plaintext are shown in Eq. 4.14-4.23 for computing 1-bit hamming distance between $L^4[0]$ and $L^1[0]$.

$$L^4[0] = (L^3[63] \& L^3[56]) \oplus L^3[62] \oplus \mathbf{K^3[0]} \oplus R^3[0] \tag{4.14}$$

$$L^3[63] = (L^2[62] \& L^2[55]) \oplus L^2[61] \oplus \mathbf{K^2[63]} \oplus R^2[63] \tag{4.15}$$

$$L^3[56] = (L^2[55] \& L^2[46]) \oplus L^2[54] \oplus \mathbf{K^2[56]} \oplus R^2[56] \tag{4.16}$$

$$L^3[62] = (L^2[61] \& L^2[54]) \oplus L^2[60] \oplus \mathbf{K^2[62]} \oplus R^2[62] \tag{4.17}$$

$$R^3[0] = L^2[0] = (L^1[63] \& L^1[56]) \oplus L^1[62] \oplus \mathbf{K^1[0]} \oplus R^1[0] \tag{4.18}$$

$$L^2[62] = (L^1[61] \& L^1[54]) \oplus L^1[60] \oplus \mathbf{K^1[62]} \oplus R^1[62] \tag{4.19}$$

$$L^3[63] = f(\mathbf{K^2[63]}, \mathbf{K^1[55]}, \mathbf{K^1[61]}, \mathbf{K^1[62]}) \tag{4.20}$$

$$L^3[56] = f(\mathbf{K^2[56]}, \mathbf{K^1[48]}, \mathbf{K^1[54]}, \mathbf{K^1[55]}) \tag{4.21}$$

$$L^3[62] = f(K^2[62], \mathbf{K^1[54]}, K^1[60], \mathbf{K^1[61]}) \tag{4.22}$$

$$L^4[0] = f(K^2[63], K^2[56], K^1[62], K^1[61], K^1[55], K^1[54], K^1[48]) \tag{4.23}$$

Because of deeper diffusion of input key during 3 rounds, 1-bit of the L^4 is dependent on 7 bits of input key requiring 2^7 guesses for creating power model. However, when 6 rounds are unrolled (6r), intermediate state after 6 rounds (L^7) is now dependent on 81 bits of input ke (including XOR-only dependencies), making CPA infeasible as 2^81 guesses must be made to create a power model and then perform CPA. Therefore, for 6r datapath, we performed CPA targeting combinational output of 3rd round with hamming weight as power model. Fig. 4.14(a) plots correlation vs time for 3-round unrolled datapath. The correct key bits (0100100) were recovered with 22000 measurements. Fig. 4.14(b) shows that there was no attack possible for 6r datapath even with 500000 measurements. Fig. 4.15(a) plots peak absolute correlation for all the key guesses vs number of measurements and we see that a successful attack is not possible with correlation curve for correct key candidate embedded deep among all the correlation curves. Fig. 4.15(b) plots MTD and SNR for the select datapaths. SNR degrades as datapath width and degree of unrolling is increased. For 6-round unrolled datapath, SNR decreases to 0.0026 showing a degradation of 63× compared to baseline bitserial datapath. MTD shows similar trend with respect to datapath width and round unrolling. No successful attack was observed for 6-round unrolled datapath architecture. This shows an improvement of at least 384× in MTD for

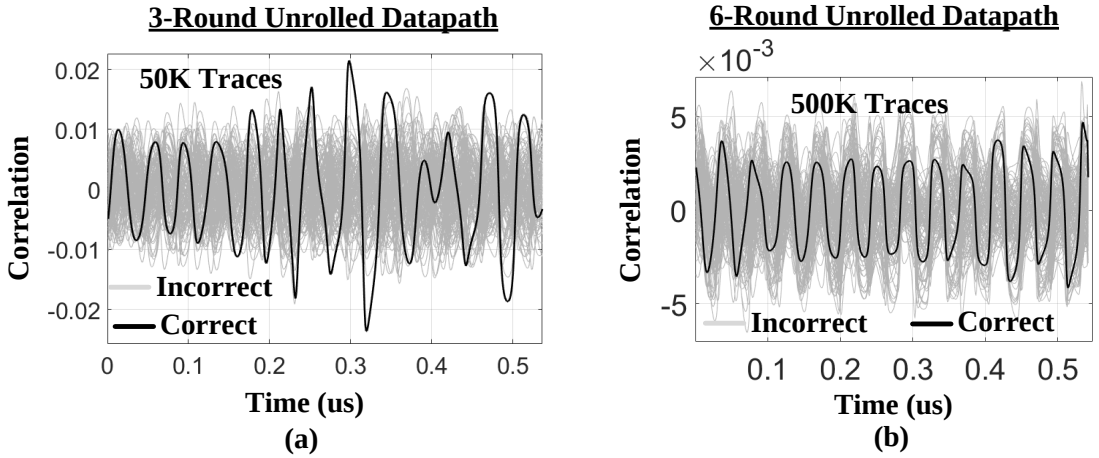


Figure 4.14: Correlation power analysis attack for round unrolled datapath with increasing degree of unrolling: (a) successful CPA for 3-round unrolled datapath, (b) no CPA attack observed for 6-round unrolled datapath even with 500K measurements.

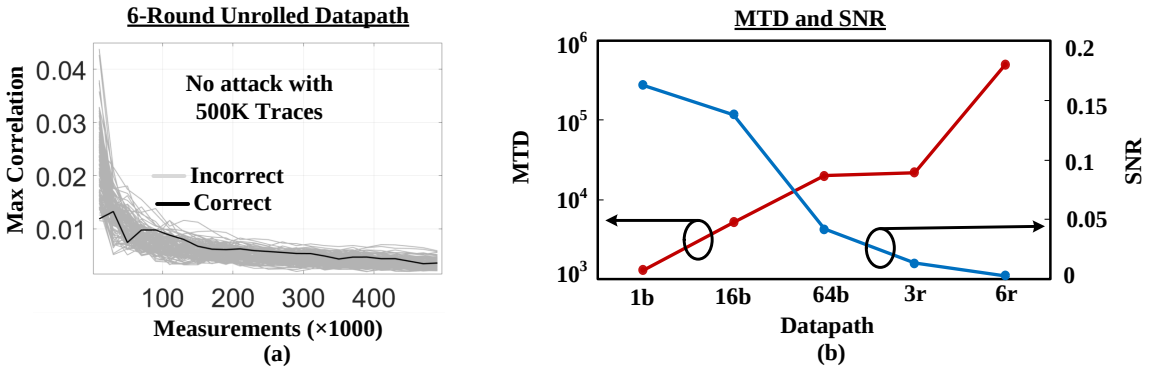


Figure 4.15: Correlation power analysis attack for round unrolled datapath with increasing degree of unrolling, (a) max correlation vs number of measurements for 6-round unrolled datapath and (b) MTD and SNR plotted for different datapath architectures. SNR decreases as the datapath width and degree of unrolling is increased. Similar trend is seen for MTD with no CPA attack for 6-round unrolled datapath indicating an increase of at least 384× with respect to bitserial datapath.

6-round unrolled datapath with respect to bitserial datapath.

Table 4.4 compares different datapaths for SIMON128 from their ASIC and FPGA implementations on Sakura-G with respect to area, performance and energy. We see that for SIMON128, a round unrolled design can offer both higher performance and lower energy while providing excellent resistance to SCA attack. Also, with respect to high performance (128-bit) and compact (8-bit) datapath implementations of Advanced Encryption Standard (AES), SIMON128 provides much higher flexibility for implementations across wide range of platforms, specifically for IoTs with much smaller area and energy footprints compared to AES. However, while choosing a specific implementation for SIMON128, one should

Table 4.4: Comparison of different datapath architectures for lightweight cipher SIMON128 and state-of-the-art AES128 encryption scheme.

		ASIC					FPGA					
	Data-path	Area (μm²)		Perf.		Energy (pJ/enc.)	Area		Perf.		Energy (nJ/enc.)	CPA (MTD)
		Reg.	Comb.	Freq. (GHz)	Latency (cycles)		Reg. (slices)	Logic (slices)	Freq. (MHz)	Latency (cycles)		
SIMON128	1b	360	208	16	4352	3113	499	525	250	4352	423	1300
	64b	336	391	16.9	68	61.7	480	757	294	68	6.5	20000
	64b, 3r	339	1111	11.6	23	38.9	481	804	223	23	1.68	22000
	64b, 6r	337	3380	7.4	12	72	481	1692	145	12	0.46	>500K
AES128	128b	830	7525	8	11	43	1000	3302	167	11	0.852	6000
	8b	856	1350	7.38	500	861	1030	1306	164	500	30	2400

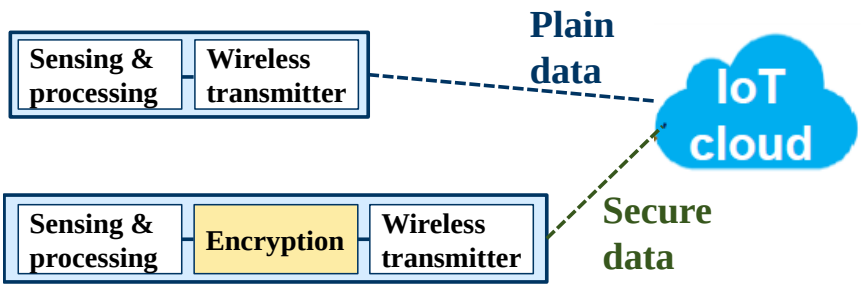


Figure 4.16: The IoT environment with IoT cloud and edge devices. An edge device with encryption engine transmits secure data to the IoT cloud.

be aware that different datapaths have different side channel leakage and if securing the sensitive secrets is of utmost importance, round unrolled datapath with a high degree of unrolling ($r \geq 6$) should be chosen for higher resistance to SCA.

4.4 Application of SIMON-128 to an Image Sensor Node

Internet of Things (IoT) is an emerging technology that envisions a world in which millions of connected objects are communicating with one another, creating a wide range of applications from smart cities, smart homes to connected vehicles [2]. One of the key drivers for the IoT environment is collection of rich information at the edge devices such as image sensors, which transmit the processed data to the IoT cloud for more sophisticated data analysis [122]. Due to the ubiquitous nature of IoT edge devices, the transmitted data often includes sensitive private, confidential, or safety critical data. To ensure data privacy and confidentiality in IoT environment, it is critical that the transmitted data from edge devices is protected against data theft or malicious tampering. Therefore, there is a need to integrate cryptographic functions into IoT edge devices and sensors [Fig. 4.16].

Since IoT edge devices have stringent resource constraints such as energy and area, complex cryptographic functions can result in huge overhead for the edge devices. For example, encryption engines with a significant complexity such as Advanced Encryption Standard (AES) engines used in high-performance processors [123, 124] are not suitable for resource-constrained platforms due to the lack of available area and/or power/energy.

Therefore, the design goal for a secure IoT edge device should target for minimum energy/area/performance overhead, as well as resistance to attacks. In the subsequent sections, we apply the optimized SIMON128 architectures to a low power image sensor node and elaborate on the power, performance, area, energy overheads along with resistance to side channel attack resistance and compare proposed SIMON128 datapaths to more conventional AES128 datapaths in terms of latency, energy, area, throughput and SCA resistance.

4.4.1 Baseline Image Sensor Node

To demonstrate the energy efficiency and throughput improvement, we apply the proposed encryption engine to an illustrative IoT edge device, a low-power image sensor node presented in [125]. The image sensor node is designed to capture image frames, and reduce the amount of the data to be transmitted by detecting the region-of-interest (ROI) and encoding the non-ROI with lower quality. As Fig. 4.17 shows, the system includes an ROI detection and coding unit and a motion JPEG encoder. The baseline image processing platform first divides each frame image into 8x8 macroblocks (MBs), each of which is processed by a moving object detection method to identify the ROI blocks in a frame. Then the ROI/non-ROI blocks are encoded differently in a ROI-based coding unit. The parameters of the processing units are jointly controlled by a rate controller to keep the data rate satisfy the target rate. The image sensor system is synthesized into an ASIC with 15nm process node. The layout of each component of the system are shown in Fig. 4.18. Area and power consumption values are listed in Table 4.5.

4.4.2 Overhead Comparison

The system overhead analysis of the image sensor system is presented as the energy and latency required per image frame, which has 320x240 resolution. As the ROI-based encoding in the sensor node reduces the data, the amount of encrypted data will generally be

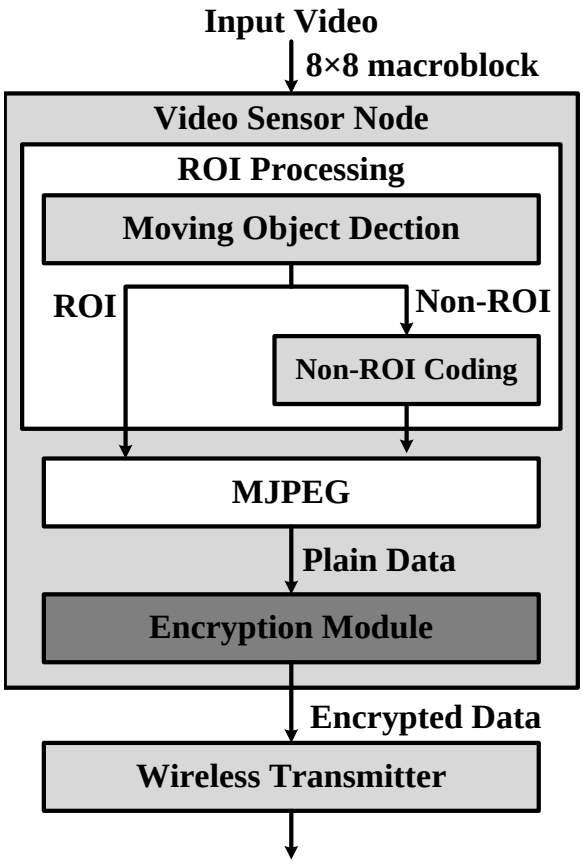


Figure 4.17: Block diagram of the image sensor node.

smaller than the original image data size. The data reduction ratio is assumed to be 10x, which is achieved for the ROI quality (SSIM) of 0.9 with typical input video frames [126]. Also, we assume pipelining with three stages (ROI processing, MJPEG encoding, and encryption), so the stage with the largest latency becomes the throughput bottleneck of the system.

Fig. 4.19 shows latency and energy of the baseline unsecured system, AES, and SIMON encryption engines. With the narrow datapath, the AES (8b) and SIMON (1b) show high latency, resulting in an increased end-to-end system latency by 65.3% and 262%, respectively [Fig. 4.20(a)]. Also, as the encryption latency is higher than the latency of unsecured image sensor, encryption becomes the throughput bottleneck of the system [Fig. 4.20(b)]. By optimizing the datapath, the latency of the SIMON engine is significantly reduced, increasing the system latency only by 1.6%. Also, as the encryption latency can be hidden by

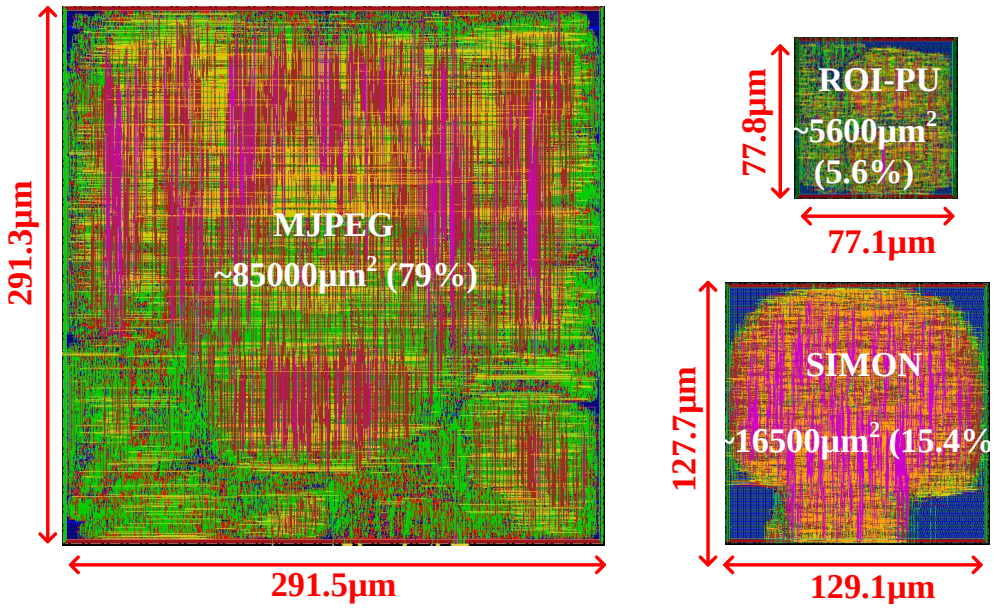


Figure 4.18: Physical implementation details for high-performance image sensor node with side-channel secure communication with NCSU FreePDK 15nm technology libraries-placed and routed layout of individual blocks (MJPEG, ROI processing unit and 64b, 6 round unrolled SIMON)

the image processing latency, the system throughput is not affected by the encryption. Fig. 4.19(b) also shows that the SIMON with 1-bit datapath consumes comparable energy to the unsecured system. With significantly reduced energy, the optimized SIMON increases the system energy only by 0.5% [Fig. 4.20(c)].

Table 4.5: Physical implementation details for high-performance image sensor node with side-channel secure communication with NCSU FreePDK 15nm technology libraries - summary of area and power consumption for individual blocks after synthesis and place & route.

Module	**Area (μm^2)**		**Power (mW)**
	synth	**layout**	
ROI processing unit	3,271	5,600	27.1
MJPEG	49,530	85,000	141
Baseline image sensor system	**52,801**	**90,600**	**168.1**
SIMON (64b, 6r)	3,717 (+7%)	16,500 (+18%)	44.4 (+26%)
Total	**56,518**	**107,100**	**212.5**

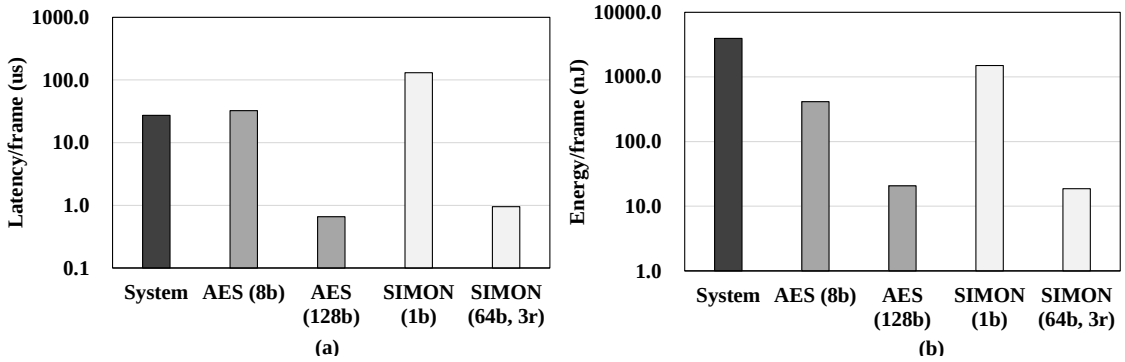


Figure 4.19: (a) Latency and (b) energy consumption of the unsecured sensor system and AES/SIMON encryption engines.

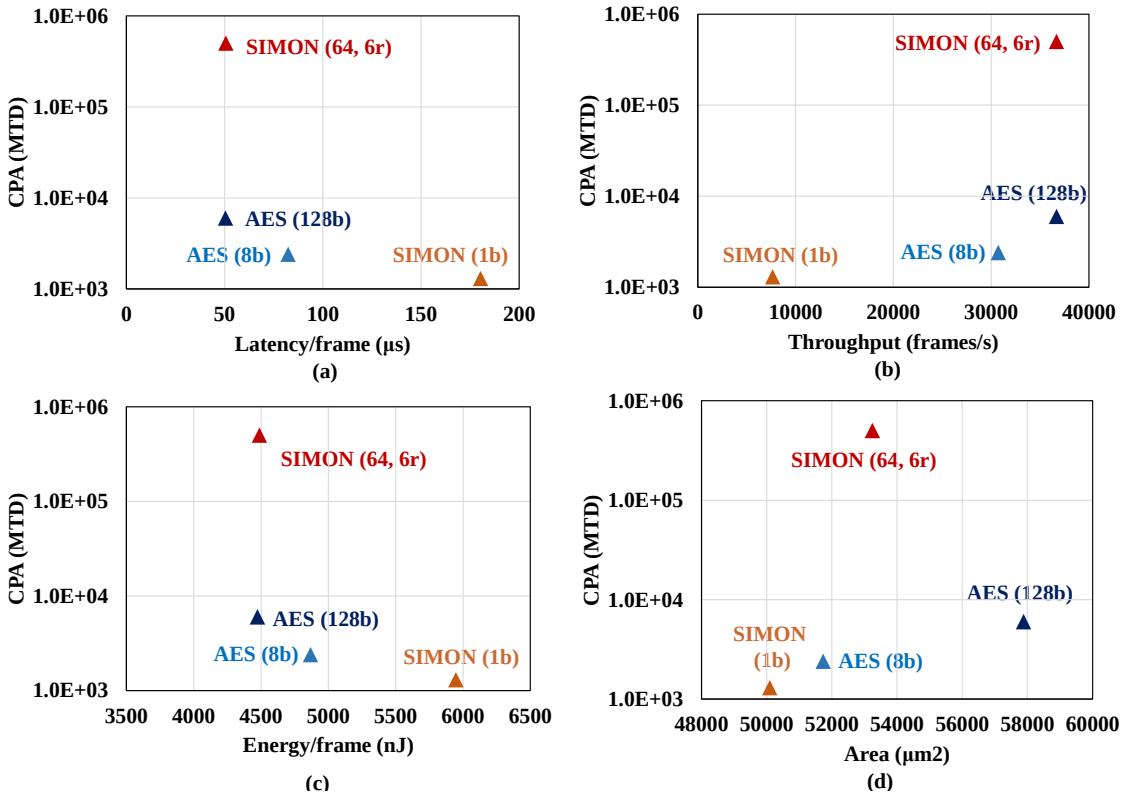


Figure 4.20: Overhead and resistance comparison of the image sensor system with four different encryption engines. (a) End-to-end latency, (b) system throughput, (c) energy, and (d) area overhead.

Although the AES engine with 128-bit datapath also yields low energy and latency overhead, its major drawback is vulnerability to SCA with relatively smaller required MTD (6,000). Moreover, it has largest area overhead among the four encryption engines, increasing the system area by 17% [Fig. 4.20(d)]. On the other hand, the optimized SIMON

achieves higher robustness to the SCA (MTD>500K), with negligible latency, throughput, energy, and area overhead (1.6%, 0%, 0.8%, and 7.5%, respectively) compared to the unsecured image sensor system.

4.5 Summary

This chapter demonstrated an optimized unrolled datapath architecture for SIMON128 to secure an image-sensor node for IoT-edge devices with minimal latency, throughput, energy, and area overheads (1.6%, 0%, 0.8%, and 7.5%, respectively). Different hardware architectures of SIMON128 targeted for low area compact design to high-performance application are explored. From datapaths synthesized in NanGate FreePDK15 standard cell library, we observe that a 3-round unrolled datapath can provide the minimal energy (80× improvement) while offering very good performance (143× better) compared to baseline bitserial datapath architecture. Moreover, because of different side channel leakage characteristics for different datapaths, choosing a datapath which leaks the least amount of information is crucial for very sensitive applications. With application to an image sensor node, we demonstrated that unrolled datapath with sufficiently high degree of unrolling can provide at least 83× higher power side channel analysis attack resistance at equivalent performance and energy efficiency with respect to traditional 128b AES engine.

CHAPTER 5

IMPROVED SCA RESISTANCE WITH RANDOM FAST VOLTAGE DITHERING

Different datapath architectures as discussed in the last chapter have varying degree of side channel leakage. However, to make the cryptographic hardware hightly resistant to side channel attacks, a countermeasure has to be designed and integrated with the encryption engines. Recently, there has been a growing interest in exploiting on-chip power management and clocking circuits to provide side channel analysis resistance [44, 46–48, 50, 81, 83–85, 127–129]. In particular, Kar et. al. [128] have demonstrated that inductive IVR with randomized control loop can reduce power side-channel leakage from a 128-bit AES engine when measured at the input of the IVR as AES supply node is not externally accessible. However, for IVRs with on-package or bond-wire based inductors [59], AES supply node remains externally accessible and hence, unprotected. Therefore, it is important to explore techniques that reduce leakage at the AES supply node (along with IVR input), especially for IVRs designed with off-chip inductors.

In this chapter, we present random fast voltage dithering (RFVD), a generic circuit level technique, for increasing P-SCA and EM-SCA resistance of AES engines [Fig. 5.1]. Instead of performing all encryptions at a constant voltage and frequency, RFVD uses a high-frequency, high-bandwidth IVR [60] to dither the voltage around the target level by randomly assigning a different voltage for each encryption. A critical path replica based all-digital clock modulation (ADCM) circuit [130] transforms the voltage variations to dithering of the clock edges to ensure correct operation while creating timing randomness between encryptions. Consequently, RFVD distorts both amplitude and timing of the AES generated power trace, thereby improving SCA resistance at the AES supply node (V_{AES}). More randomness is added by breaking 1-to-1 relation between voltage and frequency using an externally programmable trimmer inside the global modulator of ADCM

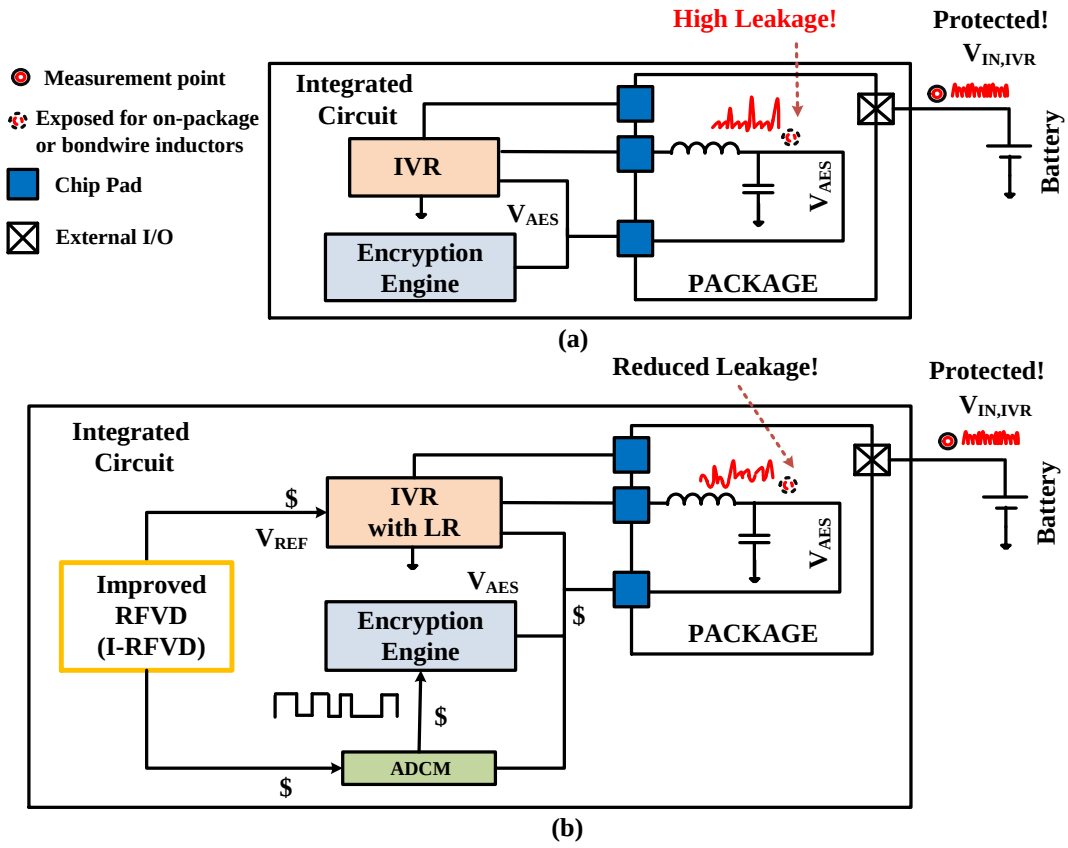


Figure 5.1: Exploiting integrated voltage regulators (IVR) and all-digital clock modulation (ADCM) for improved resistance to side channel analysis (SCA) attacks: (a) on-chip IVR with bondwire/on-package inductors and (b) on-chip integrated IVR+ADCM architecture for SCA-resistant encryption engines.

circuit (GM based frequency randomization, GM-FR) to generate different frequency levels ($<= F_{MAX}$) for a specific voltage level during encryptions, and therefore thwarting clustering-based analysis of measured traces. Moreover, RFVD is integrated with control loop randomization in IVR (IVR-LR), demonstrated by Kar et. al. [128] to reduce P-SCA leakage at the input supply node of IVR ($V_{IN,IVR}$). The IVR-LR induces additional randomness at V_{AES}, which is harnessed by ADCM to further distort the power signature at the V_{AES}.

Our prior work, the most closely related to this work, has presented an integrated inductive voltage regulator (IVR) with control loop randomization to reduce P-SCA of an AES-128 engine. An IVR isolates V_{AES} from external measurements and transforms

the power signature before it can be observed at $V_{IN,IVR}$, thereby enhancing P-SCA resistance at $V_{IN,IVR}$, but not at the V_{AES} [128]. For on-package and bondwire based inductors, the supply node of AES remains exposed/unprotected. Hence, IVR-based P-SCA protection, as presented in prior works, requires on-chip inductors to prevent external access to V_{AES}. In comparison, proposed RFVD scheme distorts the power traces at V_{AES} and transforms the distorted power trace via the IVR, improving P-SCA resistance at both V_{AES} and $V_{IN,IVR}$. Therefore, proposed scheme can enhance P-SCA resistance of a system with on-package/bondwire inductor based IVRs where both $V_{IN,IVR}$ and V_{AES} are accessible.

The RFVD is demonstrated in a 130nm CMOS test-chip that includes 128-bit high-performance (P-AES) and low-power (S-AES) AES engines powered by IVR with wire-bond inductors [60]. This chapter will present the concept of Basic and Improved RFVD (B-RFVD, I-RFVD) with key contributions highlighted below:

- First, we present basic RFVD (B-RFVD) implemented using an on-chip IVR and ADCM circuit; then describe circuit techniques to introduce additional randomness for improved RFVD (I-RFVD) scheme, namely, GM-FR and IVR-LR.
- Second, we present SCA analysis based on time and frequency domain.
- Third, we present measurement results on P-SCA resistance using RFVD including measurements on P-AES and S-AES encryption engines.
- Fourth, we present EM measurement results showing the effect of improved RFVD (I-RFVD) on EM-SCA.

The rest of the chapter is organized as follows. Section 5.1 presents system architecture; Section 5.2 and Section 5.3 will present basic and improved RFVD respectively; Section 5.4 discusses measurement setup and statistical analysis methods; Section 5.5 and Section 5.6 present the measurement results for power- and EM- side channel analysis respectively; and Section 5.7 concludes the chapter.

5.1 System Overview

Fig. 2 shows overall system architecture consisting of two datapath implementations for a 128-bit AES core powered by an inductive IVR. This section describes the circuit blocks in detail-

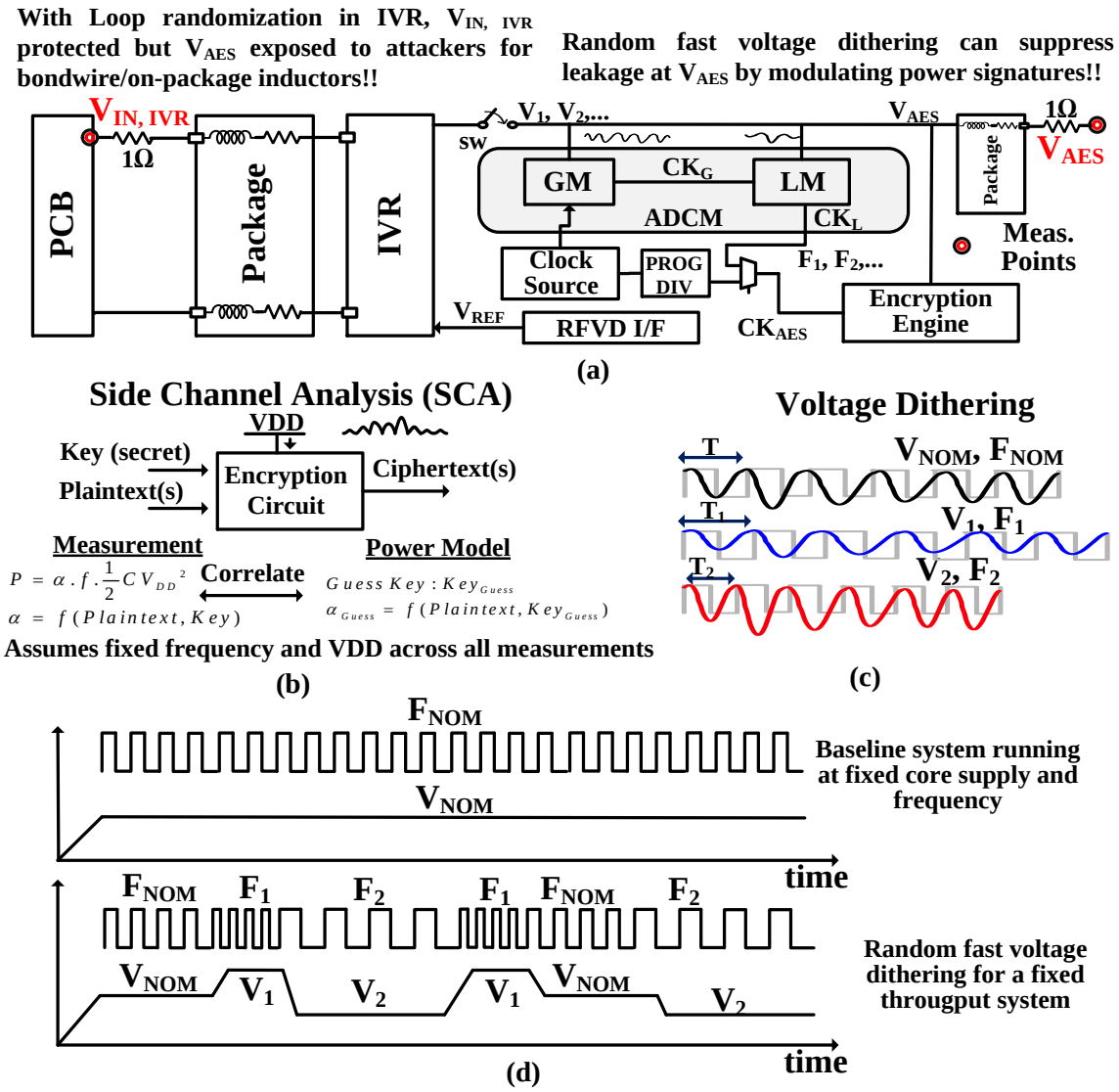


Figure 5.2: (a) Overall system architecture for RFVD, (b) supply and frequency dependence of correlation power analysis (CPA), (c) SCA leakage suppression of an AES core with RFVD, and (d) RFVD for fixed throughput encryption core.

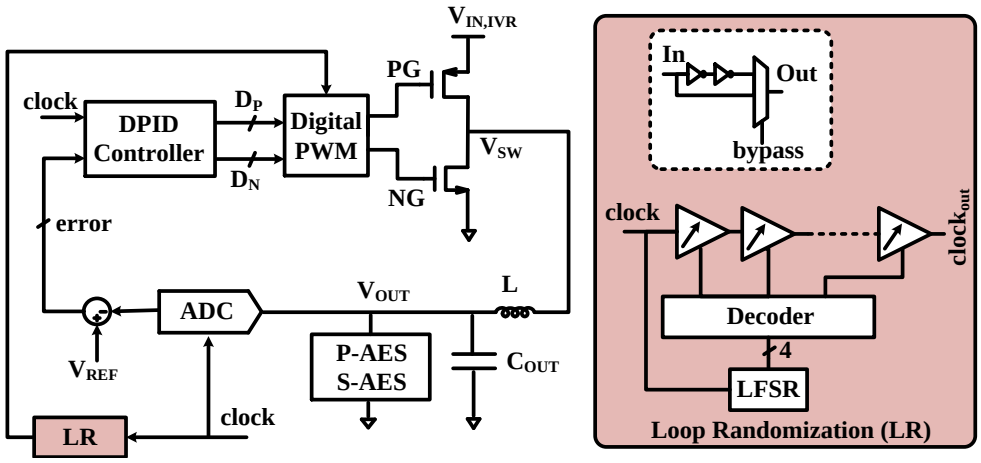


Figure 5.3: (a) Block diagram for IVR and (b) Loop randomization (LR) circuit [20].

5.1.1 Advanced Encryption Standard (AES) Designs

Two datapath architectures implemented in the testchip are parallel AES (P-AES) with 128-bit datapath and serial AES (S-AES) with 8-bit datapath. These architectures along with AES algorithm are described in detail in chapter 3.3 [Fig. 3.3].

5.1.2 Integrated Inductive Voltage Regulator (IVR)

A digitally controlled high-frequency IVR [131] with a wire-bond inductor powers the encryption core and clock modulators, [Fig. 5.3(a)]. The IVR employs a 4-bit delay-line based ADC, digital proportional-integral-derivative (DPID) controller on the feedback path to compensate for the loop and a digital pulse-width-modulator (DPWM) engine to generate control pulses for the IVR power-stage. Both ADC and DPID controller run at 250MHz and DWPM runs at 125MHz enabling multisampling ($2\times$) for 125MHz power-stage. The small inductor ($\sim$12nH), high operating frequency ($\sim$125MHz), and resistive transient assist techniques enable fast voltage transition at the output (250mV/80ns).

5.1.3 All-Digital Clock Modulation (ADCM)

The all-digital clock modulation (ADCM) circuit provides modulated clocks to the encryption cores [130]. ADCM consists of a global modulator (GM) and a local modulator (LM).

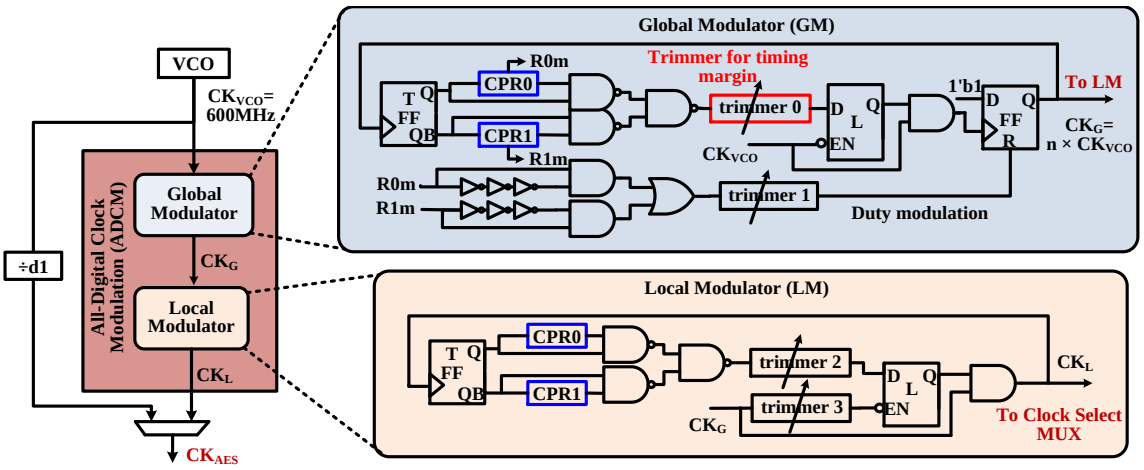


Figure 5.4: Block diagram for ADCM circuit with GM and LM utilizing critical path replicas for P-AES. ADCM when enabled supplies clock to encryption cores.

The GM has two replicas of the critical paths of the targeted encryption core (P-AES has the worst case critical path) Fig. 5.4. A high frequency VCO (600MHz) supplies the input clock (CKSRC) to GM. GM responds to any DC change or global noise in the supply by generating an output clock (CKG) matching the delay of the critical paths with resolution = TCK,SRC = 1.67ns. Two programmable trimmers are kept in GM to create extra timing margin (trimmer 0) and to modulate the duty cycle (trimmer 1) of CKG. The period of CKG is an integer multiple of $T_{CK,SRC}$. The LM also utilizes two critical path replicas and responds to local supply variations by modulating the duty cycle of its input clock (CKG), or by gating the active edges in case of large droops. Trimmer 0 inside LM can be controlled using a free running full length 5-bit linear feedback shift register (LFSR) to activate clock gating randomly. The GM and LM respond at cycle-by-cycle speed. The entire logic for GM and LM is fully synthesizable. It is placed and routed using standard physical design tools.

5.2 Basic Random Fast Voltage Dithering (B-RFVD)

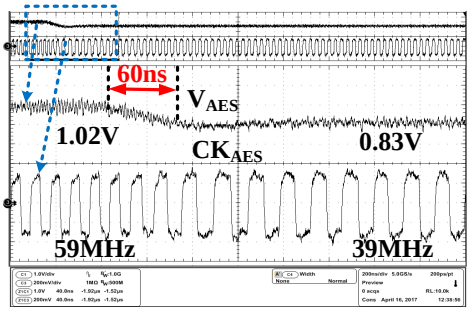
Voltage dithering has been previously used to obtain continuous wide-range dynamic voltage frequency scaling (DVFS) using a few discrete voltage-frequency (V-F) operating

points [132, 133]. The proposed basic RFVD (B-RFVD) system randomly dithers V-F around a target to distort the AES power signature while maintaining a target system throughput. B-RFVD is facilitated by IVR and ADCM. An on-chip register storing the reference word of the IVR is updated by randomly selecting one of 6 different reference values. IVR generates corresponding output level after the reference transient delay.

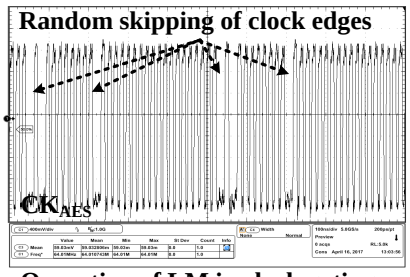
In response to the voltage changes, the ADCM adapts the output clock period to translate the voltage dithering to clock dithering. As the frequency changes continuously in lockstep with voltage during voltage transition, ADCM prevents timing error during the transition. The B-RFVD scheme is realized by characterizing IVRs output voltage versus ADCMs output clock frequency. The operating voltage is randomly changed in shorter time-scales (after every 20 encryptions), which also shifts the instantaneous period of AES clock, such that average number of encryptions performed over a sufficiently long duration (average throughput) remains same. Fig. 5.5(a) shows the measured voltage-frequency response of the ADCM module for a constant VCO frequency (600MHz). Fig. 5.5(b) shows the measured response of the ADCM to IVR output level transition from 1.02V to 0.83V within 60ns. Corresponding ADCM output clock frequency varies from 59M to 39MHz.

(a)

Voltage (mV)	834	868	880	890	940	1020
Freq. (MHz)	39.2	42	45.3	49.7	53.5	59.3



(b)



Operation of LM in clock gating and duty modulation mode

(c)

Figure 5.5: (a) Table listing all 6-quantized voltage and frequency levels, (b) worst case voltage transition from 1.02V to 0.834V occurs in 60ns with ADCM modulating clock, even during the transition, ensuring correct operation, and (c) Additional random shifts added to clock edges from LFSR controlled LM trimmer.

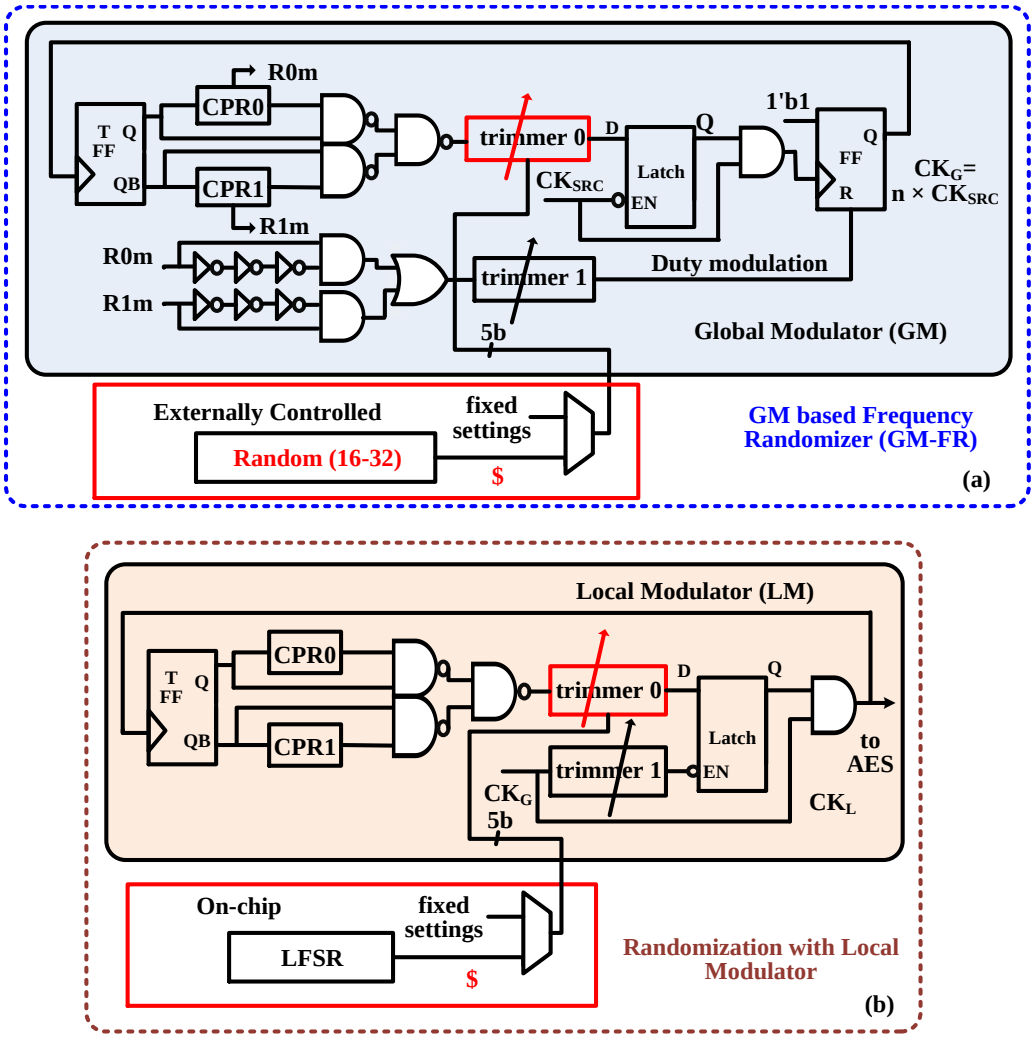


Figure 5.6: Block diagram for ADCM circuit: (a) trimmer 0 inside GM can be externally programmed to randomize the frequency corresponding to a voltage level and (b) randomly triggered duty modulation and clock gating modes with LFSR controlled trimmer 0 in LM.

Fig. 5.5(c) shows measured waveform for LM output clock when LFSR controlled trimmer is activated.

5.2.1 Impact of B-RFVD on SCA

B-RFVD randomly changes V_{AES} leading to random shifts in clock edges between operations (changes in F_{AES}) and random changes in the amplitude of power signatures [Fig. 5.7(a)]. The clock modulators also respond to transient noise in the AES supply node, introduced by load circuits (AES) and/or injected by the IVR, resulting in additional shifts

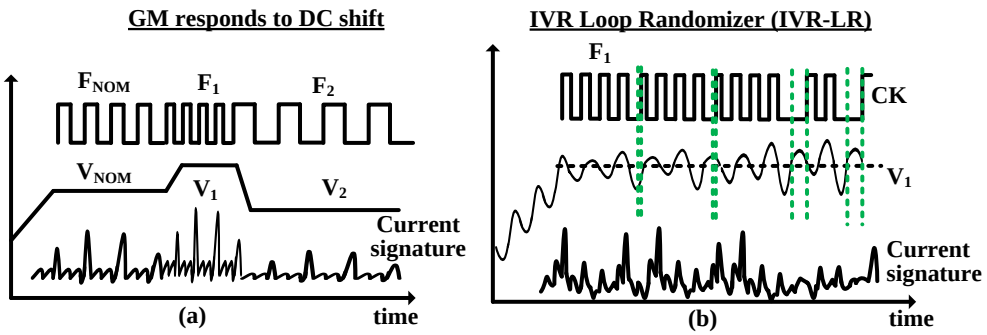


Figure 5.7: Sources of randomization from B-RFVD scheme: (a) GM dithers clock freq. in response to voltage dithering and responds to any global noise/DC shift, (b) IVR-LR not only adds noise in V_{AES} but also interacts with GM and LM in ADCM.

in the clock edges. Randomness from LM can be injected by utilizing on-chip LFSR controlled trimmer 0 which triggers LM in duty modulation and clock gating mode [Fig. 5.8 (a) & (b)]. With B-RFVD, power signatures across different encryptions are randomized de-correlating measured power from the input vectors across different encryptions.

5.3 Improved Random Fast Voltage Dithering (I-RFVD)

One drawback with B-RFVD scheme is that voltage and frequency have 1-to-1 relationship and the measured power traces can be clustered in corresponding V-F groups using cross-correlation in time-domain or highest frequency component, which should correspond to frequency of operation, in frequency domain. The clustered traces can be separately analyzed. With cluster analysis, maximum resistance that can be obtained from B-RFVD scheme would ideally (in absence of any other embedded time/voltage noise in the system) be equal to number of V-F pairs. To improve the SCA resistance offered by B-RFVD scheme, 1-to-1 relationship between V-F pair can be broken with GM-FR and IVR-LR. The difference between B-RFVD and I-RFVD with respect to ADCM circuit is the way trimmer 0 inside GM is exploited to further randomize the frequency and interaction between IVR loop randomizer (IVR-LR) and ADCM circuit inducing more amplitude and frequency randomizations depending on the noise generated by the IVR-LR. These improvements are

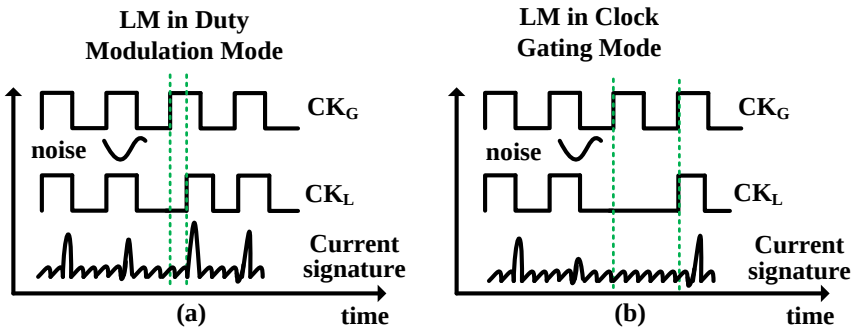


Figure 5.8: Sources of randomization from B-RFVD scheme: (a) LM modulates duty cycle of output clock, and (b) LM skips some of the clock edges in presence of random noise.

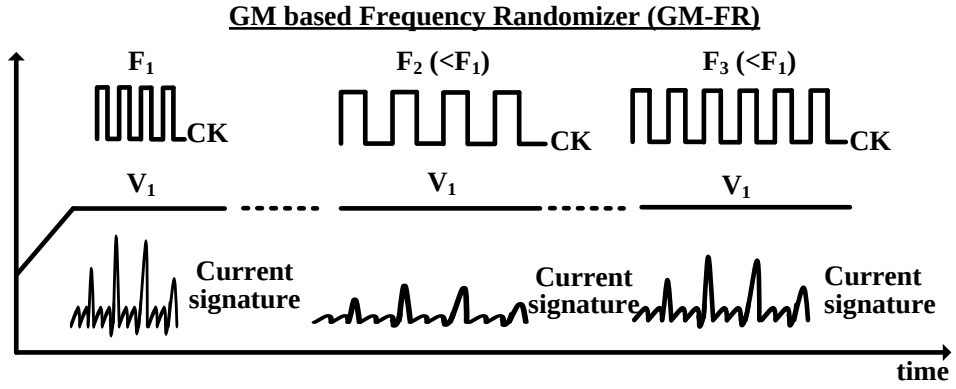


Figure 5.9: Additional sources of randomization from I-RFVD scheme - externally controlled trimmer 0 producing different clock freq. levels breaking 1-to-1 V-F correspondence.

described as below

5.3.1 Impact of Global-Modulator based Frequency Randomization (GM-FR) on SCA

Trimmer 0 inside GM has 32 taps with 16 taps enabled to create adequate timing margin. When GM-based frequency randomization (GM-FR) is enabled, higher number of taps are enabled with a random number generator outputting uniformly distributed random numbers between 16 and 32. This makes sure that atleast 16 taps (default case) are enabled while some taps are randomly added. With higher number of taps enabled, GM output clock (CKG) is now mapped to different frequency level F ($\leq$F1) for voltage level V1 [Fig. 5.9]. This not only makes clustering difficult but also injects additional misalignment within each V-F group.

5.3.2 Impact of IVR Loop Randomizer (IVR-LR) on SCA

IVR induces both small-signal and large-signal transformation from local supply node of AES (V_{AES}) to input of IVR ($V_{IN,IVR}$). However, there is not much impact of IVR at V_{AES} for IVR+AES system and power signature at V_{AES} shows similar SCA characteristics as a standalone AES system. In prior works [128], we demonstrated that with random delays added on the feedback path of the IVR through a loop randomizer (IVR-LR) [Fig. 5.3(b)], IVR-LR randomizes both small-signal and large-signal transformations and protects $V_{IN,IVR}$. However, the impact of IVR-LR on V_{AES} wasnt analyzed. IVR-LR injects random noise at the output (V_{AES}) [Fig. 5.7(b)] which is harnessed by ADCM circuit to add random misalignment in clock edges and therefore power signatures are further randomized. Random noise injected by IVR-LR is a function of LR frequency and is higher for higher LR frequency. In our experiments, LR is operated at 250MHz, same as IVR feedback loop.

I-RFVD, with different sources of randomization reduce the correlation between measured power traces to the power model by translating changes in AES supply to unpredictable misalignment in the power traces and therefore reduces the side channel leakage.

5.4 Measurement Setup and SCA Methods

Fig. 5.10(a) shows the die-photo of test-chip consisting of IVR, ADCM circuit and AES engines fabricated in 130nm CMOS. Fig.5.10(b) shows measurement setup for SCA characterization. Plaintext and keys are loaded from a computer using Arduino firmware. An external trigger signal starts the encryption and ciphertext is read back to validate the correct operation. 1 voltage setting (out of 6) is randomly (uniform) chosen in the software after every 20 (RFVD interval) encryptions. The RFVD interval should be chosen so that adversary cant reveal any information within that interval while ensuring low performance overhead (settling time for IVR reference transients). Fig. 5.11(a) shows the test-board

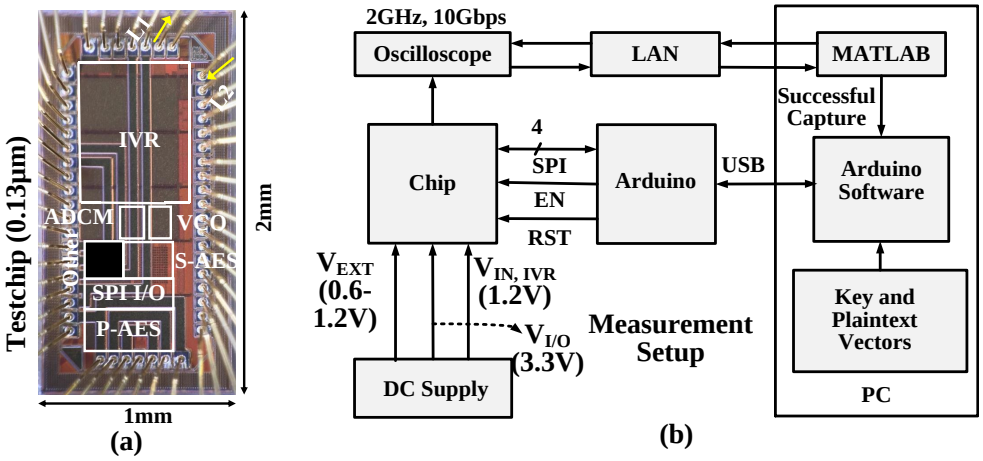


Figure 5.10: (a) Die photo of IVR+ADCM+AES system, and (b) measurement setup.

designed to measure the side channel activity for both power and EM signatures.

5.4.1 Acquisition of Power Signatures

Power signatures are measured at V_{AES} across 1 resistor using Tektronix DPO5204 oscilloscope (2GHz bandwidth, 10Gbps max sampling freq.) at 1Gbps sampling rate and 500MHz bandwidth.

5.4.2 Acquisition of EM Signatures

EM signatures are captured with a non-invasive EM probe - large loop probe from Beehive Corporation (probe 100C, tip diameter of 1, loop diameter 0.85, 3dB bandwidth of 50MHz, 1st resonance freq. of 500MHz) [98]. Fig. 5.11(b) shows the pad (I/O) diagram for the test-chip. For capturing EM signatures, pads for AES VDD/VSS are targeted while placing the EM probe [Fig. 5.11(c)].

5.4.3 Measurement Conditions

3 different systems characterized for SCA leakage are described as below:

1. **Baseline**: AES powered from IVR, still running at fixed clock frequency (F_{NOM}=∼50MHz @0.89V).

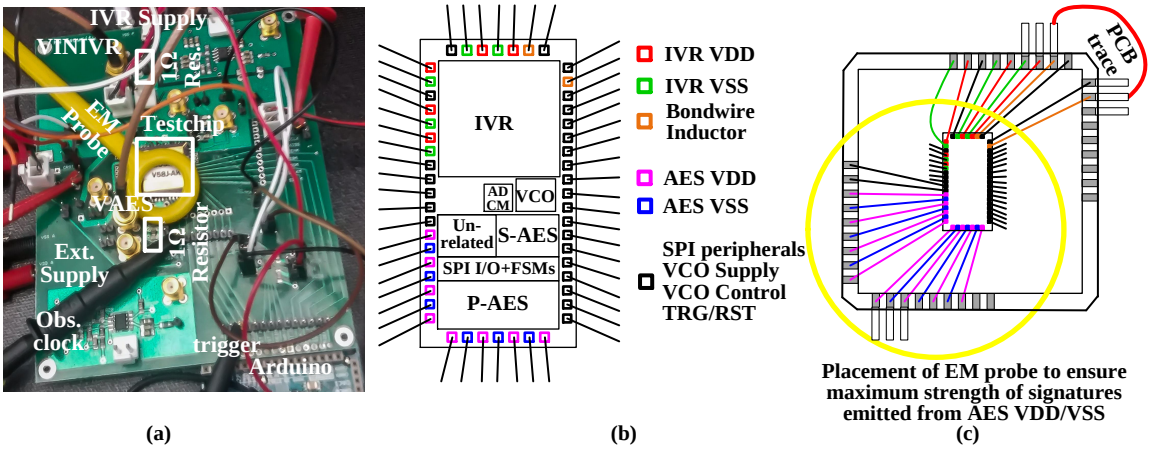


Figure 5.11: (a) Test-board for measuring side channel activity, (b) pad diagram for the test-chip, and (c) placement of EM probe for capturing EM signatures generated by local VDD and VSS nodes of AES.

2. **B-RFVD**: AES powered with IVR and running with ADCM modulated clock with IVR output varied randomly in regular interval (after every 20 encryptions).

3. **I-RFVD**: RFVD+GM-FR+IVR-LR system with GM-FR (GM trimmer 0 settings randomly varied between 16 and 31) and IVR-LR (LR runs at 250MHz) enabled.

5.4.4 Side Channel Analysis (SCA) Methods

Test Vector Leakage Assessment(TVLA)

In addition to regular (1st) order TVLA test discussed in chapter 3.2.3, higher order TVLA test is also carried out. Higher order TVLA tests consider 2^{nd}, 3^{rd}, 4^{th} and 5^{th} statistical moments [134]. Regular t-test can be carried out using Eq. 3.8. For higher order TVLA, the mean and variance can be replaced with higher order central moments as described in Eq. 5.1 to 5.5. Higher-order TVLA tends to perform better results in presence of uncorrelated noise/countermeasures.

$$(1^{st}\,order) \quad \mu = M_1, \qquad \sigma^2 = CM_2 \tag{5.1}$$

$$(2^{nd}\,order) \quad \mu = CM_2, \qquad \sigma^2 = CM_4 - CM_2^2 \tag{5.2}$$

$$(3^{rd}\,order) \quad \mu = SM_3 = \frac{CM_3}{(\sqrt{CM_2})^3}, \qquad \sigma^2 = \frac{CM_6 - CM_3^2}{CM_2^3} \tag{5.3}$$

$$(4^{th}\,order) \quad \mu = SM_4 = \frac{CM_4}{(\sqrt{CM_2})^4}, \qquad \sigma^2 = \frac{CM_8 - CM_4^2}{CM_2^4} \tag{5.4}$$

$$(5^{th}\,order) \quad \mu = SM_5 = \frac{CM_5}{(\sqrt{CM_2})^5}, \qquad \sigma^2 = \frac{CM_{10} - CM_5^2}{CM_2^5} \tag{5.5}$$

where CM_n is the n^{th} order central moment. The values for μ and σ^2 can directly be used in Eq. 3.8 to perform higher order t-test. In our experiments, we capture 120,000 signatures for both power and EM traces for performing TVLA for all measurement conditions. These measured traces are divided in two subsets of 60000 measurements to carry out two experiments to ensure repeatability of TVLA leakage. t-test is performed in both time and frequency domains.

Correlation Power/EM Analysis (CPA/CEMA)

Both CPA and CEMA are utilized for key recovery attacks. Chapter 3.2.2 describes these methods in detail. Upto 1 million power and EM signatures are captured for CPA and CEMA attacks.

5.4.5 Postprocessing and Alignment Techniques

Measured traces are filtered with zero-phase bandpass filters (5MHz) to remove out-of-band noise. A wider bandpass filter with 40MHz band (30MHz to 70MHz) centered at F_{NOM} ($\sim$50MHz) is also analyzed. Filtered traces were aligned using cross-correlation to remove initial delay (Δt) arising from use of external trigger [Fig. 5.12]. TVLA and CPA/CEMA is performed on the aligned signatures. Fig. 5.13(a) shows measured raw

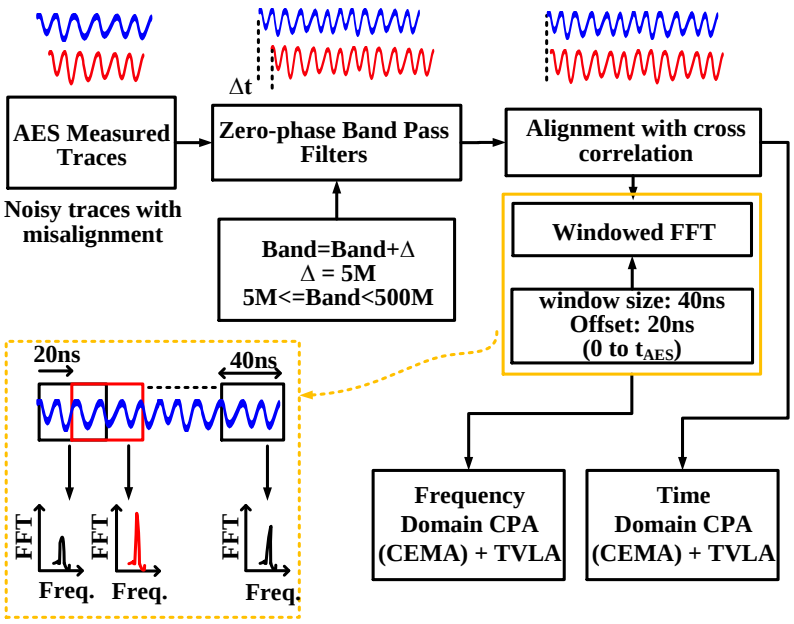


Figure 5.12: Post-processing, alignment techniques and side channel analysis in time and freq. domain with sliding window based FFT.

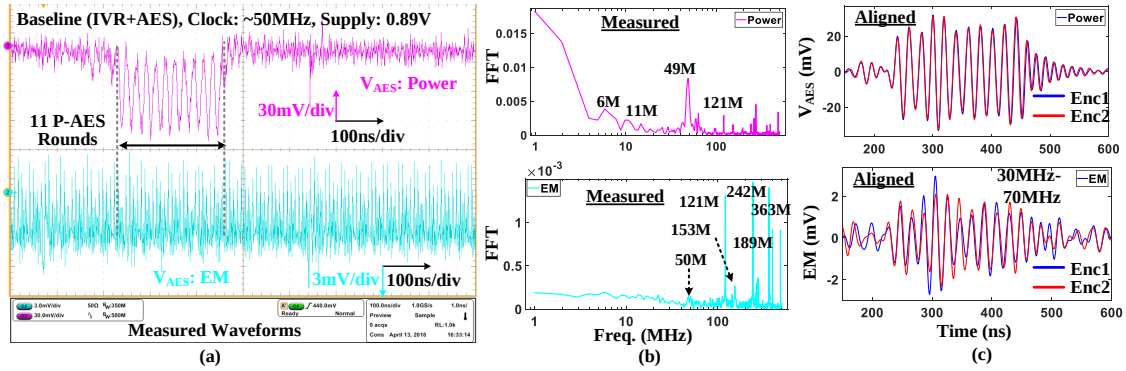


Figure 5.13: Filtering and alignment of measured waveforms for baseline IVR+P-AES: (a) measured raw waveforms for power/EM signatures, (b) FFT of measured waveforms, and (c) filtered with 30-70MHz band and aligned waveforms.

power/EM signatures for baseline P-AES design. All 11-rounds of operation are observed in both signatures. FFT of power signature shows highest peak at AES clock (∼50MHz) [Fig. 5.13(b)]. FFT of EM signature shows weaker strength compared to power signature. However, EM signature shows large number of peaks with higher signal strength at non-AES clock frequencies (IVR switching freq. and its harmonics). Fig. 5.13(c) shows aligned waveforms for 2 encryptions.

Fig. 5.14(a) shows measured waveform for I-RFVD system. The noise injected from

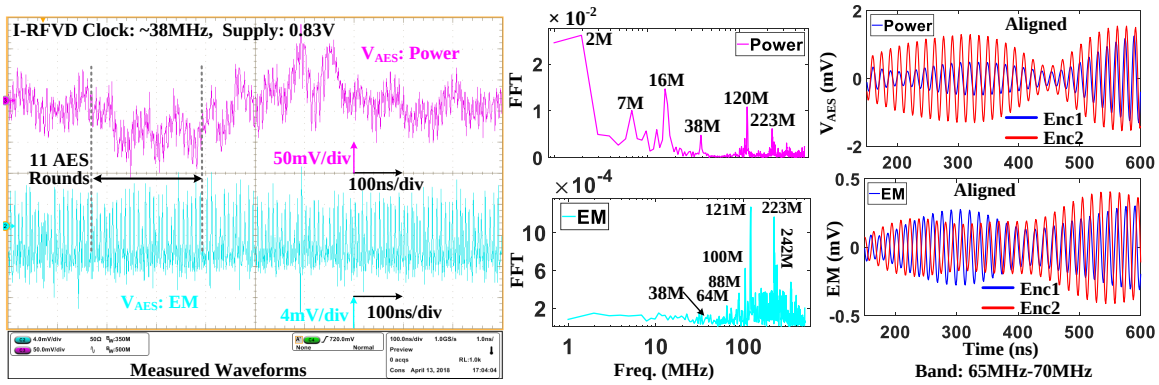


Figure 5.14: Filtering and alignment of measured waveforms for P-AES with I-RFVD: (a) measured raw waveforms for power/EM signatures, (b) FFT of measured waveforms, and (c) filtered with 65-70MHz band and aligned waveforms.

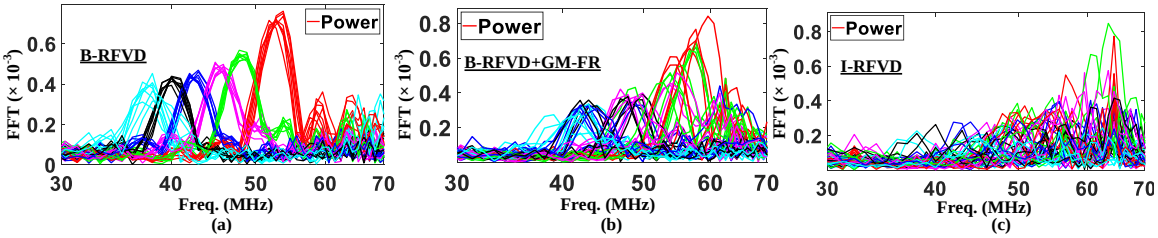


Figure 5.15: Effect of different randomizations on spectral content of measured power signatures: (a) B-RFVD system, (b) B-RFVD+GM-FR system, and (c) I-RFVD system.

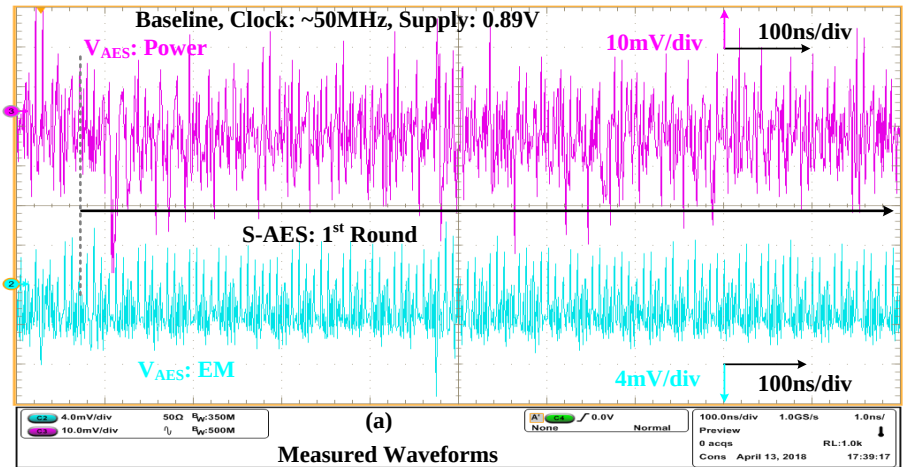


Figure 5.16: Measured raw waveforms for power/EM signatures for baseline IVR+S-AES system.

IVR-LR can be observed. Fig. 5.14(b) show corresponding spectral content. We observe that FFT peak corresponding to AES clock (39MHz @V_{AES}=0.83V) is weaker now and a FFT peak corresponding to IVR switching freq. ($\sim$ 125MHz) along with its harmon-

ics is also present. With RFVD, the measured traces correspond to different voltage and frequency levels, so cross-correlation based alignment for waveforms filtered with wider band (30-70MHz), as expected, show very poor alignment. However, with narrow bandpass filter (5MHz), most of the waveform is aligned as shown in Fig. 5.14(c) as narrow bandpass filter target frequency components in a narrow band. Fig. 5.15 shows frequency spread for captured signatures for different measurement conditions with signatures for a V-F pair color coded with a single color. For I-RFVD system, it is very difficult to cluster the measured traces in corresponding V-F pair based on frequency components. Fig. 5.16 shows measured power/EM signatures for standalone S-AES design.

5.5 Measured Results: Power Side Channel Analysis (P-SCA)

TVLA and CPA analysis are performed on measured power signatures to quantify the improvement in SCA resistance for both P-AES and S-AES engines.

5.5.1 Parallel AES (P-AES)

Unlike prior works [128], TVLA analysis is performed in both time and frequency domains. Frequency domain analysis eliminates misalignment effects. Additionally, windowed FFT with sliding window, optimal window size/offset increases signal-to-noise ratio (SNR) in the window of interest as frequency components from the unrelated parts of the signature are not considered which improves the TVLA peak and reduces CPA MTD. TVLA and CPA results in time/freq. domains are analyzed below:

Test Vector Leakage Assessment (TVLA) for P-AES

Baseline System: Baseline IVR+P-AES system shows significant leakage with 120K measurements with t-statistic of 197. Unprotected design is expected to leak significantly. Fig. 5.17 (a) and (b) plot t-statistic for baseline system across time and frequency respectively. Fig. 5.18 compares t-statistic for the same in time and freq. domain. There are certain

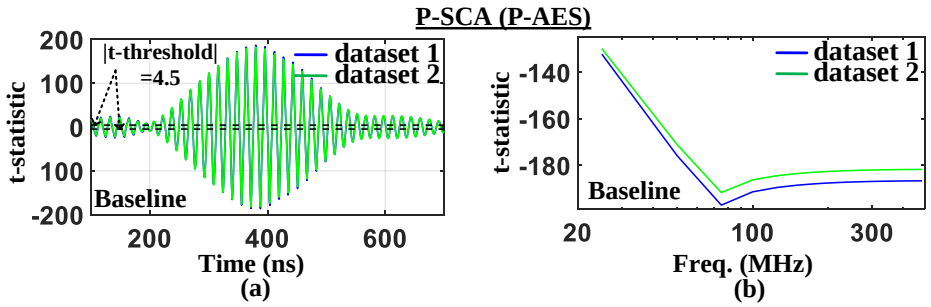


Figure 5.17: TVLA analysis results for baseline (IVR+AES) system. t-statistic plotted across: (a) time, and (b) freq.

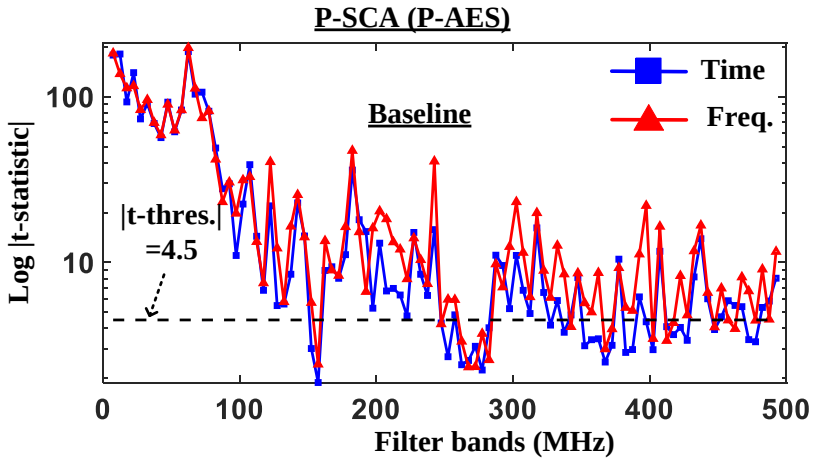


Figure 5.18: Comparison of time and freq. domain TVLA leakages for baseline IVR+AES system.

bands which have higher leakage in frequency domain and vice-versa. TVLA results from time domain and frequency domain are combined as described in Eq. 5.6. To detect leakages in the presence of time/voltage noise and with countermeasures, higher-order TVLA analysis is performed. Fig. 5.19 shows leakages for order=1, 2, 3. Baseline system has significant leakages for order=2 and order=3. For comparing across different systems, the TVLA leakages for all orders (1 to 5) are combined as described in Eq. 5.7.

$$|t-statistic| = max(|t-statistic(time), |t-statistic(freq.)|) \tag{5.6}$$

$$|t-statistic| = max(|t-statistic(order)|), \qquad order = 1 \ldots 5 \tag{5.7}$$

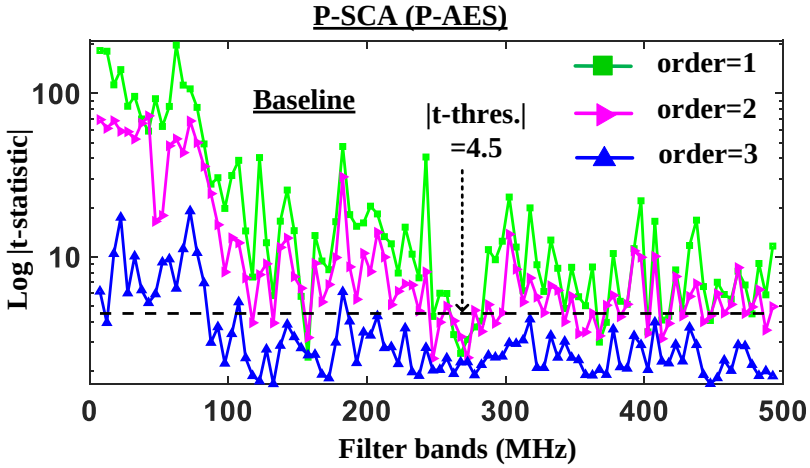


Figure 5.19: Comparison of time and freq. domain TVLA leakages for baseline IVR+AES system.

B-RFVD and I-RFVD systems: When B-RFVD is enabled, t-statistic is significantly reduced (from 197.1 to 37.9, 5.2×). Interestingly, 2nd order TVLA shows highest leakage as higher order TVLA analysis is mean-free, therefore, any changes in mean value of power consumption due to B-RFVD and any changes in measurement conditions over the duration of the experiment are eliminated. Additionally, B-RFVD system shows increased TVLA leakages in higher bands [Fig. 5.20]. B-RFVD system has 6 different AES clock frequencies corresponding to 6 V-F pairs, these clock frequencies and their harmonics are potential leakage frequencies. For I-RFVD system, the TVLA leakage is still present [Fig. 5.20] but greatly reduced (5.28) indicating a 37.3× reduction with respect to baseline system. Like B-RFVD system, higher leakage is observed for 2nd order TVLA in time domain with only two bands (380-390MHz) leaking. Table 5.1 summarizes time/freq. domain leakages for order=1, 2, 3 for all systems. Overall, when all sources of randomization are enabled for I-RFVD system, the TVLA leakage reduces by 37.3× and leakages across most of the filter bands go below the t-threshold of 4.5.

Table 5.1: Summary of higher order TVLA analysis for P-AES with baseline, B-RFVD and I-RFVD systems.

Design	order=1		order=2		order=3		Max	
	Time	Freq.	Time	Freq.	Time	Freq.	Time	Freq.
Baseline: IVR+AES	186.9	197.1	72.8	71.8	9.2	19	186.9	197.1
B-RFVD	21.5	29.7	37.9	33.9	24.9	30.4	37.9	33.9
I-RFVD	3.85	4.37	5.28	4.99	3.45	2.7	5.28	4.99

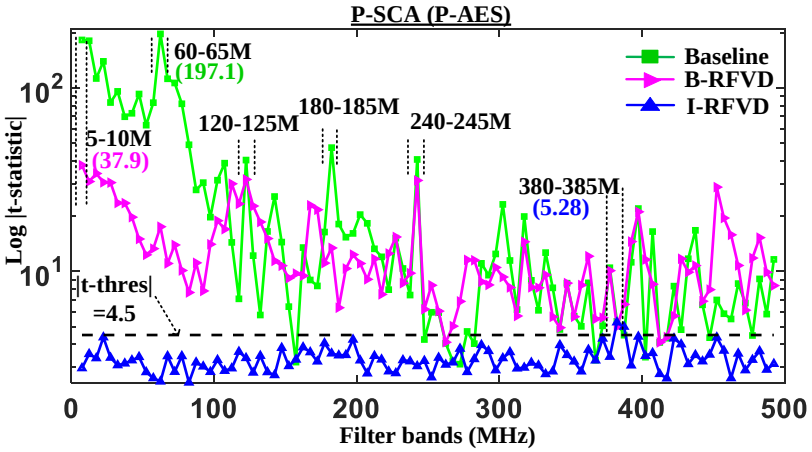


Figure 5.20: Comparison of time and freq. domain TVLA leakages for baseline IVR+AES system.

Correlation Power Analysis (CPA) for P-AES

Correlation power analysis is performed on the measured power signatures. To find the filter band with the highest leakage, a corr. (correlation) ratio metric is defined as described in chapter 3.2.2. Corr. ratio is > 1 for a successful attack and $<=1$ when there is no attack. Corr. ratio is expected to increase with increasing number of measurements. Corr. ratio is computed for all systems across filter bands and MTD is computed for the band with the highest corr. ratio.

Baseline System: Fig. 5.21(a) shows time domain CPA for baseline system for 10K measurements. Similarly, Fig. 5.21(b) plots correlation vs freq. for correlation freq. analysis (CFA). Correct key guess for byte 9 is successfully revealed with only 5600 traces in time domain and 1300 in freq. domain [Fig. 5.23(a)]. Corr. ratio is plotted against filter bands in Fig. 5.22. It shows highest leakage in 15-20MHz filter band. Freq. domain attack

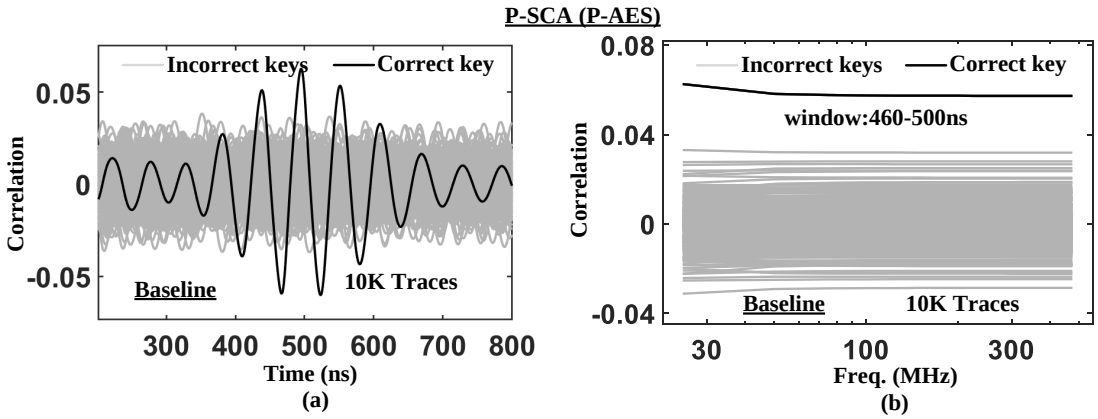


Figure 5.21: CPA analysis results for baseline (IVR+AES) system in time and freq. domains. Correlation plotted against (a) time, and (b) freq.

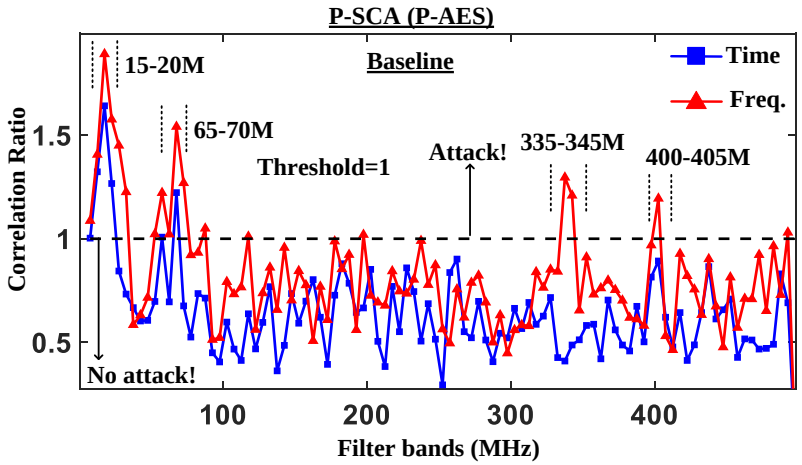


Figure 5.22: Comparison of time and freq. domain TVLA leakages for baseline IVR+AES system.

has significantly higher leakage than time domain attack, also evident with $>4\times$ smaller MTD for CFA. Additionally, freq. domain attack shows leakages in higher filter bands which is not present in time domain attack.

B-RFVD and I-RFVD systems: B-RFVD system could not be attacked with CPA using a wider bandpass filter (30-70 MHz) around nominal AES clock freq. ($\sim$50MHz) in time domain, even with 1 million measurements. However, when narrow bandpass filters are applied, the B-RFVD system could be attacked with 400K measurements required in time domain (60-65 MHz band) and only 30K measurements needed in freq. domain [Fig. 5.23(b)]. For I-RFVD system, CFA shows an attack with 900K measurements required

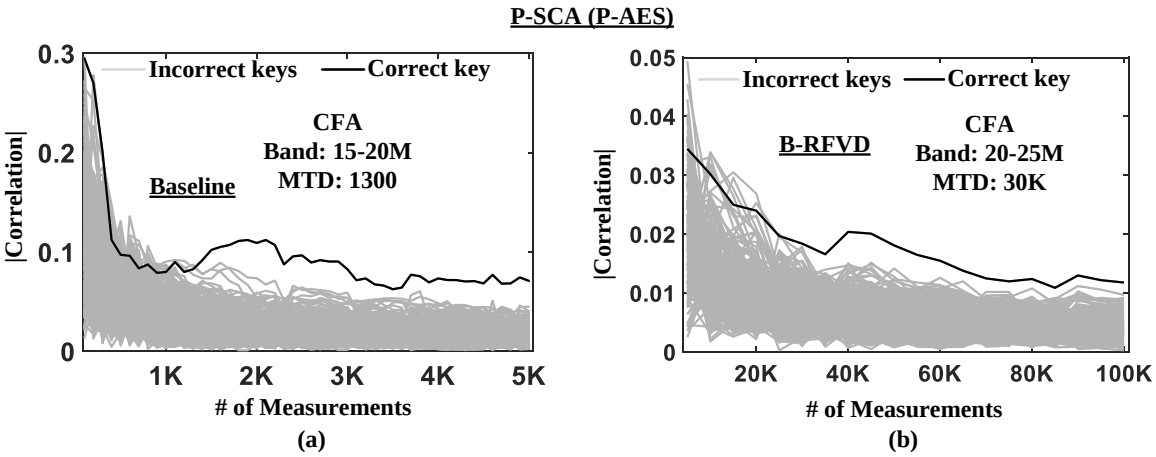


Figure 5.23: MTD plot for correlation frequency analysis (CFA) for P-AES (a) baseline, and (b) B-RFVD system.

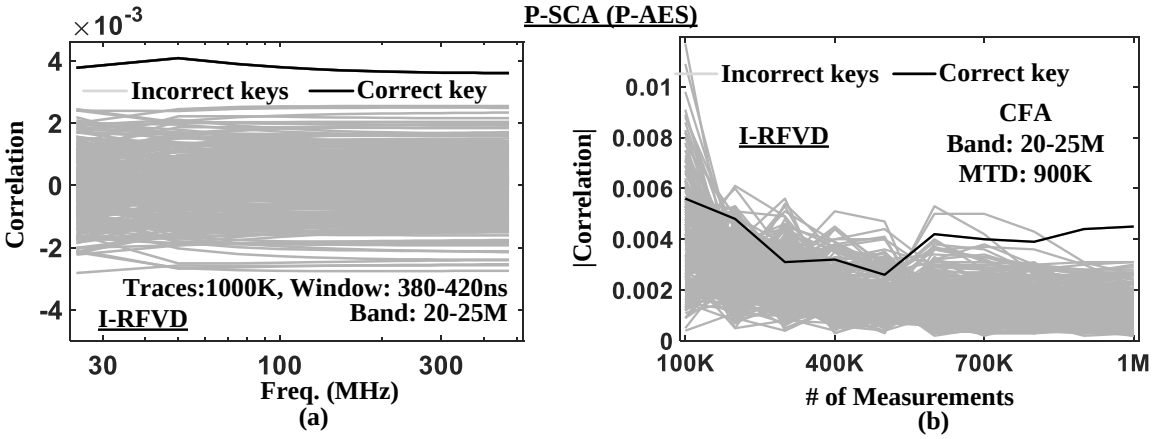


Figure 5.24: CFA results for I-RFVD system: (a) correlation against freq., and (b) MTD plot.

indicating an increase of 642× with respect to baseline design [Fig. 5.24 (a & b)]. There was no successful time domain attack. Like TVLA, only few bands are leaking for CFA.

Overall, when all the sources of randomization are enabled for P-AES, measured power signatures show a reduction of 37.3× in TVLA leakage and increase of 642× in CPA MTD.

5.5.2 Serial AES (S-AES)

To understand the impact of proposed I-RFVD scheme on different architectural implementations of 128-bit AES algorithm, both TVLA and CPA analysis is performed on the measured signatures for S-AES. The analysis results are discussed as below:

Test Vector Leakage Assessment (TVLA) for S-AES

Baseline System: Baseline system shows significant TVLA leakage (peak = 101.3 in time domain, as shown in Fig. 5.25. However, it is significantly smaller than P-AES (101.3 vs 197.1 respectively). S-AES has lower algorithmic noise (all the bytes are processed serially) compared to P-AES (higher algorithmic noise). However, because of very small voltage drops, it is difficult to detect rounds and therefore, it is difficult to align the rounds/clock cycles with cross-correlation compared to P-AES where all the rounds are very distinct. Additionally, since TVLA leakage is analyzed in the middle rounds of encryption operation, S-AES has significant clock drift where clock jitter is accumulated over many clock cycles from the start of the trigger (encryption latency of 502 cycles for S-AES). P-AES doesnt have clock drift issue due to shorter encryption latency (11 cycles).

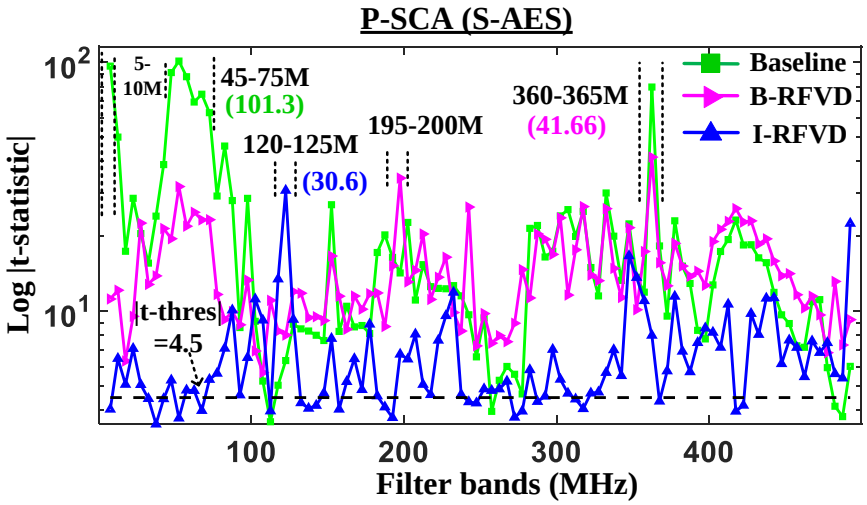


Figure 5.25: Log of —t-statistic— plotted against filter bands. S-AES shows significant leakage even for I-RFVD system.

Table 5.2: Comparison of high order TVLA leakages for order=1, 2, 3 for baseline, B-RFVD, and I-RFVD systems for S-AES.

Design	order=1		order=2		order=3		Max	
	Time	Freq.	Time	Freq.	Time	Freq.	Time	Freq.
Baseline	101.3	91.1	50.4	40.8	20.8	10.5	101.3	91.1
B-RFVD	24.3	41.66	24.2	31.7	7.65	22.28	24.3	41.66
I-RFVD	13.3	22.5	25.3	30.6	11.6	26.6	25.3	30.6

B-RFVD and I-RFVD systems: With B-RFVD, t-statistic is significantly reduced (from 101.3 to 41.66, 2.43× reduction). For I-RFVD system, the S-AES engine still leaks significantly (2^{nd} order TVLA peak of 30.6) across multiple bands indicating limited reduction in TVLA peak (3.33×) compared to baseline system [Fig. 5.25]. Table 5.2 summarizes the TVLA leakages for S-AES across time and freq. domains for order=1, 2, 3 for all the systems.

Correlation Power Analysis (CPA) for S-AES

Byte 3 is found to be having the smallest MTD with respect to baseline system and is therefore targeted for CPA attack across all systems.

Baseline System: Baseline system for S-AES shows very small MTD in freq. domain (MTD=2100) [Fig. 5.26)].

B-RFVD and I-RFVD systems: When B-RFVD is enabled, MTD for S-AES increases to 700K (by 333× with respect to baseline) indicating significantly reduced leakage with respect to CPA [Fig. 5.27(a)]. For I-RFVD system, MTD further increases to 900K (428× increase) with respect to baseline system [Fig. 5.27(b)]. In summary, even though S-AES leaks significantly across all systems with respect to TVLA, MTD for CPA increases by 428×.

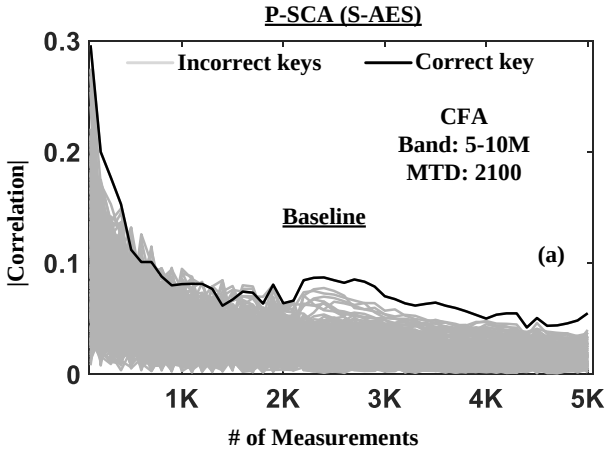


Figure 5.26: CFA results for S-AES. MTD plots for: (a) baseline, (b) B-RFVD, and (c) I-RFVD systems.

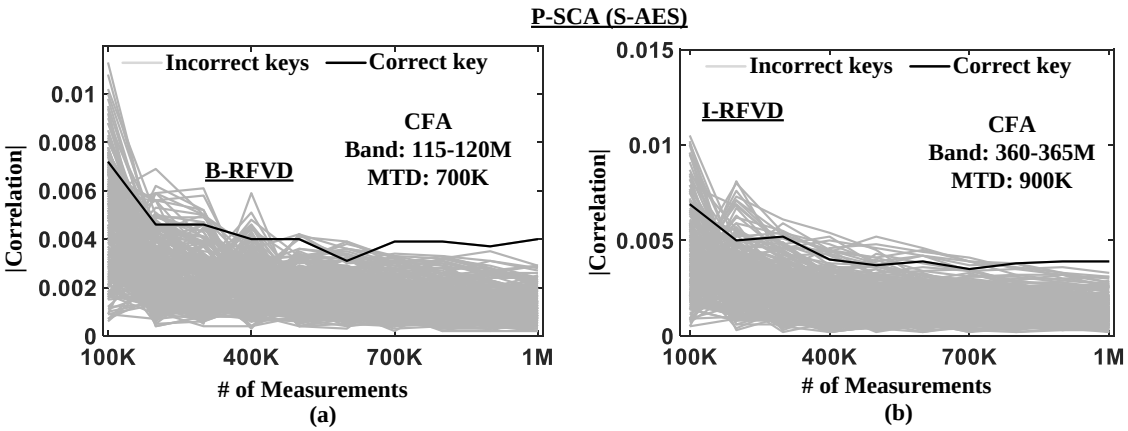


Figure 5.27: CFA results for S-AES. MTD plots for: (a) B-RFVD, and (b) I-RFVD systems.

5.6 Measured Results: EM Side Channel Analysis (EM-SCA)

Electromagnetic emanations from CMOS devices and on-chip, on-package PDN network have been shown to carry multiple, unintentional side channel signals [5] which can be exploited to break proven countermeasures targeting power side channel. [135] demonstrated that IVR-LR can also mask EM signatures generated by AES in the proximity of IVR inductor due to constant switching of the power-stage and inductor current. We investigate how the proposed B-RFVD and I-RFVD schemes impact EM side channel analysis (EM-SCA) attacks near AES VDD/VSS pads.

5.6.1 Test Vector Leakage Assessment (TVLA)

TVLA for P-AES

Fig. 5.28 plots t-statistic for P-AES against filter bands for baseline, B-RFVD and I-RFVD systems. As expected, baseline has the highest t-statistic (97.9) with 120-125 MHz (IVR switching freq.) highest leaking band. With B-RFVD, the TVLA peak reduces to 33 (2.97$\times$ reduction). Both baseline and B-RFVD show very high TVLA leakages across most of the bands indicating presence of multiple leakage sources. For I-RFVD system, the TVLA peak is 8.3 (2^{nd} order TVLA, freq. domain). This shows a reduction of 11.8$\times$ with respect

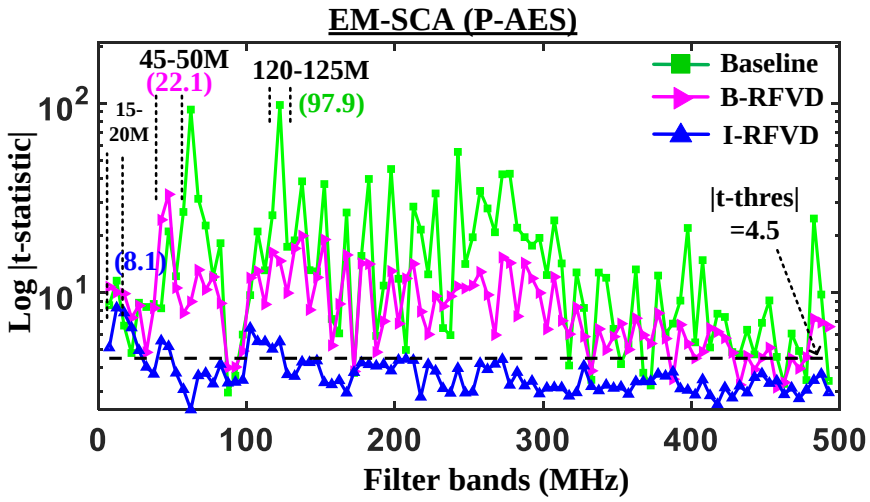


Figure 5.28: —t-statistic— plotted against filter bands for EM signatures. P-AES shows highly reduced leakage for I-RFVD system.

to baseline system.

TVLA for S-AES

Fig. 5.29 plots t-statistic for S-AES across filter bands for baseline, B-RFVD and I-RFVD systems. Baseline has the highest t-statistic (78) with 120-125 MHz highest leaking band. With B-RFVD, the TVLA peak reduces only slightly to 49.3 (1.58× reduction). For I-RFVD, the TVLA peak is 8.92 (2^{nd} order TVLA, freq. domain) indicating a reduction of 8.8× . Like P-AES, S-AES also leaks significantly across the entire spectrum for baseline, B-RFVD and I-RFVD systems.

5.6.2 Correlation EM Analysis (CEMA)

CEMA for P-AES

Fig. 5.30(a) shows MTD plot for I-RFVD system. The MTD required for successful CEMA is 900K with 45-50MHz filter band [11.3× higher than baseline]. Even though baseline systems have very different MTD for CPA and CEMA, I-RFVD shows same MTD.

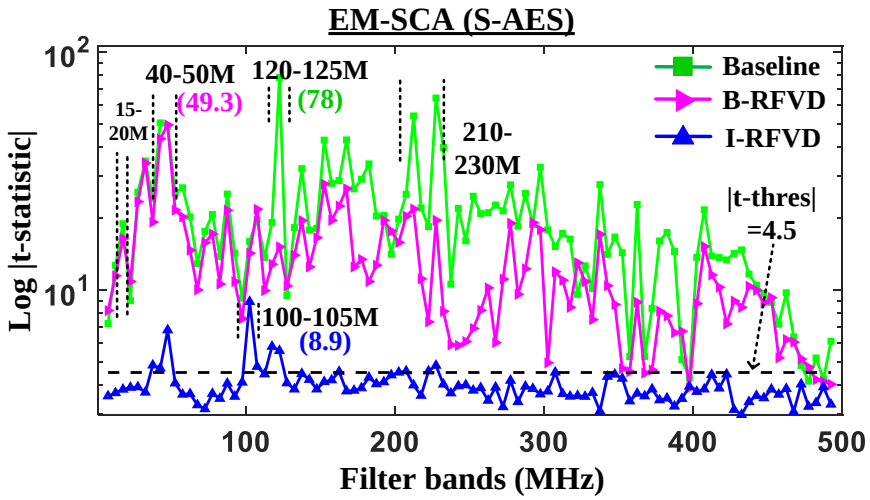


Figure 5.29: —t-statistic— plotted against filter bands for EM signatures. S-AES shows significant leakage even for I-RFVD system.

CEMA for S-AES

Fig. 5.30(b) shows MTD plot for I-RFVD system. The measurements required for a successful CEMA is only 400K for 5-10 MHz band [improvement of only 2.5× with respect to baseline, Table 5.3]. Therefore, with I-RFVD, CEMA for S-AES has much smaller MTD than CPA.

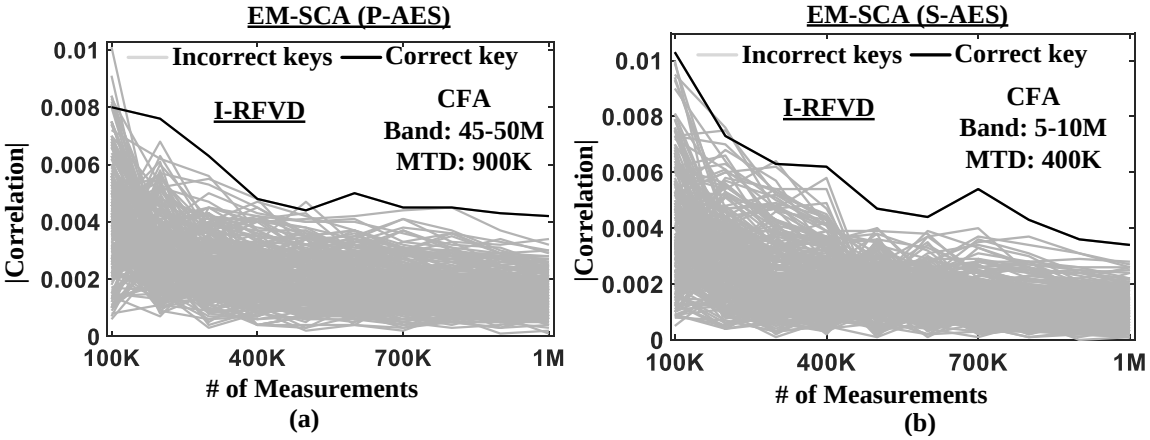


Figure 5.30: CEMA for I-RFVD system for: (a) P-AES, (b) S-AES.

5.6.3 Comparison of P-SCA and EM-SCA

Results presented in chapter 5.5 and 5.6 have shown that both power and EM signatures can be captured to perform a successful key recovery attack. An adversary can follow the path of least resistance and choose power/EM side channels based on their relative success to break the proposed countermeasures. This Section compares P-SCA and EM-SCA with respect to TVLA peaks and MTD required for a successful CPA/CEMA attack.

The extent of TVLA leakage is quantified with respect to highest peak for —t-statistic— and minimum-traces-to-detect-leakage (MTDL, $|t-statistic| \geq 4.5$). Table 5.3 lists TVLA peak/MTDL and CPA/CEMA MTD for P-AES/S-AES across all measurement conditions. We observe that for unprotected baseline P-AES, P-SCA performs much better than EM-SCA. However, when different sources of randomization are enabled which directly affect the power consumption in amplitude and time, EM-SCA starts performing equivalent to/better than P-SCA. TVLA peak and MTDL both show significant side channel leakages for EM-SCA which are not present for P-SCA for the I-RFVD system.

A slightly different trend for S-AES is seen where TVLA peak leakage with EM-SCA is considerably lower compared to P-SCA for most cases as well as for I-RFVD system. However, TVLA MTDL show similar behavior as P-SCA while CEMA MTD when countermeasures are enabled is observed to be significantly less compared to CPA MTD.

Table 5.3: Summary of all measured results for P-AES and S-AES with respect to power/EM analysis.

	P-AES						**S-AES**					
	Power			**EM**			**Power**			**EM**		
System	**CPA MTD**	**TVLA Peak**	**TVLA MTDL**	**CEMA MTD**	**TVLA Peak**	**TVLA MTDL**	**CPA MTD**	**TVLA Peak**	**TVLA MTDL**	**CEMA MTD**	**TVLA Peak**	**TVLA MTDL**
Baseline	**1.3K**	**197.1**	**20**	**80K**	**97.9**	**100**	**2.1K**	**101.3**	**60**	**160K**	**78**	**140**
B-RFVD	**30K**	**37.9**	**1.5K**	**300K**	**33**	**2K**	**700K**	**41.7**	**1K**	**300K**	**49.3**	**1K**
I-RFVD	**900K**	**5.28**	**25K**	**900K**	**8.3**	**12K**	**900K**	**30.6**	**4K**	**400K**	**8.9**	**4K**

5.6.4 Overheads of the Proposed Scheme

Performance Overheads

For B-RFVD, the performance overhead is computed using fixed system throughput. The average operating freq. for B-RFVD is same as the baseline case, however, there is some performance degradation due to finite transition time of IVR (60ns after every 20 encryptions, throughput reduces from 578Mbps to 571Mbps, 1.3% degradation). For I-RFVD, the system is run at $\leq F_{MAX}$ with GM-FR. e.g., for nominal case, with varying GM trimmer 0 settings, $\sim$5 freq. levels (49.7MHz to 37.5MHz) are generated leading to -14.4% performance degradation on an average. With IVR-LR, F_{MAX} for nominal case decreases from 49.7MHz to 49.1MHz (1.2% degradation, ADCM recovers some performance degradation by clock adaptation compared to [128]).

Power Overheads

The power consumption for AES operating at 49.7MHz @0.89V is 13.1mW. The measured power overheads due to ADCM circuit and B-RFVD scheme are 291µW (2.9%), and 380µW (3%) respectively. For I-RFVD, with GM-FR, since average freq. of operation is reduced, power reduces (-14.4% @49.7MHz, 0.89V). IVR-LR contributes 5% additional power.

Area Overheads

ADCM circuit (including B-RFVD blocks and GM-FR) consumes 11106µm2 area while IVR-LR occupies 2135 µm2 (total 6.6% of AES area).

Comparison with Existing SCA Countermeasures

Table 5.4 compares I-RFVD with prior work on increasing SCA resistance, focusing on circuit/logic level countermeasures which are similar in nature and have small overheads.

Table 5.4: Comparison of proposed I-RFVD scheme with existing countermeasures.

Metric		This Work	JSSCC'18 [128]	VLSI'15 [29]	ISSCC'09 [21]
Countermeasure Technique		Improved Random Fast Voltage Dithering	Integrated Voltage Regulator	Charge Recovery Logic	Switch Capacitor Current Equalizer
Technology		130nm	130nm	65nm	130nm
AES power		13.1mW @49.7MHz	10.5mW @40MHz	138mW @1.32GHz	33mW @100MHz
Design Overheads	Area	6.6%	1%	+25%	33%
	Power	-3.5%	+5%	-30%	20%
	Perf.	-17.4%	-3.33%	0%	-50%
# of Measurements		1,000,000	100,000	1,000,000	10,000,000
SCA Analysis Method(s)		CPA, CEMA, TVLA	CPA, TVLA	DPA	DPA
Supply Node Protected		V_{AES}, $V_{IN,IVR}$	$V_{IN,\ IVR}$	$V_{IN,\ IC}$	$V_{IN,\ IC}$

Architecture/algorithm-level techniques such as masking and threshold implementations eliminate leakage however are very different in nature and have very high overheads [26, 28] and therefore havent been compared with. Unlike the prior work by Kar et. al. [[128], I-RFVD greatly reduces side channel leakage at both $V_{IN,IVR}$ and V_{AES} nodes. I-RFVD can be used in conjunction with other SCA countermeasures based on on-chip switched capacitor [21] and charge recovery logic [29] to further improve SCA resistance. The proposed I-RFVD based countermeasure is essentially an information hiding countermeasure. However, due to its generic nature and low complexity it can also be combined with any leakage elimination countermeasure such as masking and threshold implementations, which on their own have been shown to be susceptible to higher order attacks [26, 28], to further improve the SCA resistance.

5.6.5 Discussion

Proposed I-RFVD scheme relies on randomization of amplitude and timing of acquired power/EM signatures and therefore, offers only mitigation against SCA attacks, unlike threshold implementation and masking-based countermeasures which eliminate leakage [26, 28]. However, the advantage of I-RFVD scheme is its less complexity and genericity making it easily integrable with any underlying cryptographic circuit without any need

for modification. We have performed experiments on hardware implementations of AES algorithm only and observed significantly different SCA leakage characteristics for P-AES and S-AES. S-AES due to its serial datapath (8-bit) has higher signal-to-noise ratio with respect to CPA/CEMA where a byte is targeted for attack at a time. However with respect to TVLA, all bits that are switching at a time are considered as signal (128-bit for P-AES and 8-bit for S-AES) indicating higher SNR during the targeted round for P-AES (1-cycle) and lower SNR for S-AES (16-cycles for SBOX operation) as the signal is temporally spread due to 8-bit datapath. This leads to higher TVLA leakage for P-AES for the baseline system vs S-AES. However, due to spreading of TVLA leakage for S-AES across multiple cycles, I-RFVD scheme and randomization-based countermeasures in general are not that effective with respect to TVLA as randomization will have different impact on each of these clock cycles, with some cycles still leaking significantly more even when other cycles have significantly reduced leakage with B-RFVD and I-RFVD systems. Therefore, for encryption schemes such as lightweight ciphers [101], public key encryption algorithms (ECC, RSA), the proposed countermeasure may not be as effective as they leak over multiple cycles. Since, I-RFVD induces noise in the amplitude of power signatures with pseudo-random pattern via IVR-LR and ADCM circuits, more advanced attacks (template, machine/deep learning) can be performed with a profiling step to detect the pattern and reduce the effect of I-RFVD scheme. Similarly, leakage power analysis attacks [136] can be investigated as leakage power only depends on the state of the circuit and is not dependent on the frequency of operation rendering frequency randomization ineffective. Similarly, even though authors have employed very extensive filtering schemes consisting of narrow bandpass filters across a wide frequency range in both time and frequency domains, the optimal linear filter can be obtained with a profiling step [137] which may improve the attack methods presented in this chapter. It will be interesting to develop better attack methods in future to break the I-RFVD scheme compared to the attack methods presented here. We also plan to develop theoretical models for the proposed schemes to predict and correlate measured

results with theoretical simulations/estimations.

5.7 Summary

The chapter demonstrates enhanced power/EM side channel analysis attack resistance of encryption engines using RFVD enabled by on-package inductor based high frequency IVR with loop randomizations and all-digital clock modulation. With SCA analysis performed on power/EM signatures captured from a test-chip fabricated in 130nm CMOS, we observe that even though proposed I-RFVD scheme can suppress side channel leakage present in frequency bands in proximity of AES clock, higher/lower frequency bands still tend to leak sensitive information, specifically via EM signatures which are emanated from multiple sources. However, the proposed scheme can be easily integrated on-chip without much area, power/performance overheads and provide substantial reduction in both power (upto 37.3$\times$ reduction in TVLA leakage and 642$\times$ increase in CPA MTD) and EM side channel leakage (upto 11.8$\times$ reduction in TVLA leakage and 11.3$\times$ increase in CEMA MTD).

CHAPTER 6
FAULT ATTACK MITIGATION WITH ALL-DIGITAL CLOCK MODULATION CIRCUIT

The prior works to prevent FIA for a cryptographic ASIC hardware accelerator with timing error detection circuits are primarily based on simulation studies [95, 96] and do not present experimental (hardware) results. This work considers a high-speed and fully-synthesizable ASIC implementation of ADCM circuit [Fig. 5.4] [130] with 130nm CMOS and demonstrates fault mitigation with measured results. ADCM adapts to both DC and AC variations in power supply to generate an output clock for the target digital core implementing 128-bit AES (AES-128) algorithm using 8-bit serial datapath (S-AES). In this chapter, we will first present a methodology to inject supply glitches without any assumption about accurate timing (cycle-by-cycle) of the AES operations. We then demonstrate that with ADCM circuit, one can no longer inject faults with supply glitches even after 10-million encryptions across varying operating conditions (voltage and VCO frequency, temperature variations). We further show that in extreme operating conditions, ADCM stops generating any clock edges leading to complete failure of AES operation, therefore no exploitable faults can be injected.

6.1 System Overview and Implementation

The proposed system consists of an ASIC implementation of a 128-bit AES engine with 8-bit serial datapath (S-AES) as described in Fig. 3.3(b) and ADCM circuit [Fig. 5.4] [138]. A glitch injection circuit consisting of externally controllable resistor elements is integrated on-chip to inject supply glitches of variable height and width [Fig. 6.1]. For ADCM circuit, a 32-tap programmable trimmer (trimmer 0) controlled with 5-bit SEL_TM signal adds some margin for timing in addition to critical path delay while another programmable

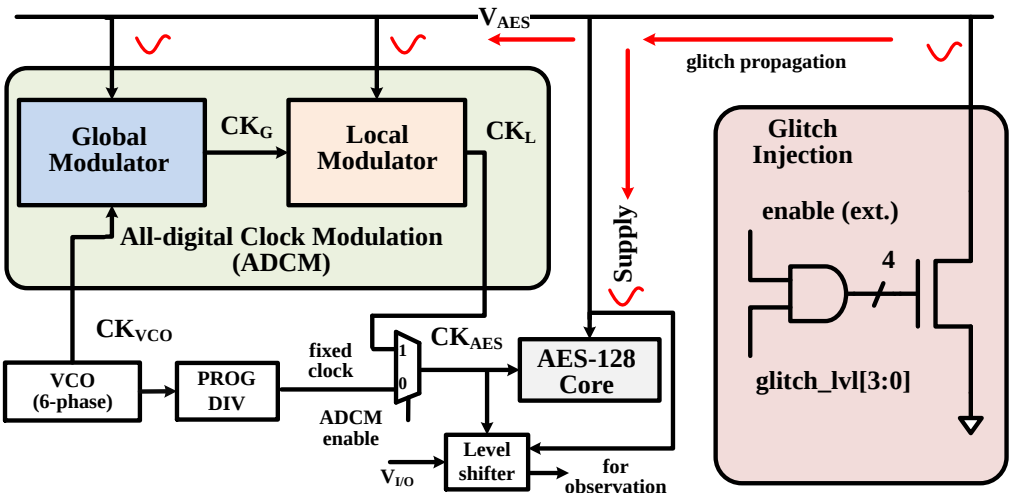


Figure 6.1: System architecture of ADCM circuit to prevent supply glitch and temperature variations-based fault attacks for a 128-bit AES encryption core.

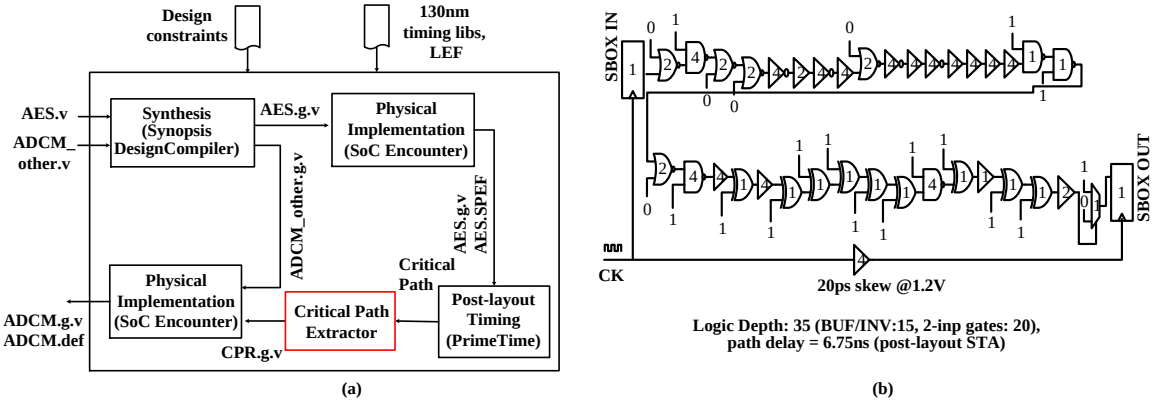


Figure 6.2: (a) Fully synthesizable design flow to implement ADCM circuit and (b) worst case timing critical path for S-AES extracted from post-layout STA.

trimmer (trimmer 1) is used to get the desired duty cycle. Moreover, Both GM and LM use sense-amplifier (SA) based flip-flops and latches to minimize metastability conditions. Unlike existing timing error prevention circuits [43, 72], ADCM circuit (GM) can respond to DC changes in supply voltages making it ideal for implementing dynamic voltage and frequency scaling algorithms on-chip [100, 129]. The entire logic for GM and LM is fully synthesizable. Gate-level netlist for all critical path replicas (CPR0..3) is extracted using a critical path extractor script from post-layout static-timing-analysis (STA) and is integrated with rest of the GM/LM gate-level netlist before it is placed and routed using standard physical design tools [Fig. 6.2 (a) & (b)].

6.2 Experimental Setup

The same testchip that we presented in Chapter 5 is used to carry out FIA experiments. The relevant components that are used for FIA work is marked in Fig. 6.3 (b). Table 6.1 provides a summary for the testchip. Fig. 6.3 (a) shows the measurement setup. An external start signal starts the encryption and ciphertext is read back for validation and DFA [Fig. 6.4].

An on-chip circuit with 4 NMOSs (binary sized - W, 2W, 4W, 8W) is used to induce supply glitches [Fig. 6.1. All NMOSs can be turned on/off with a 4-bit external glitch level (glitch_lvl[3:0]) signal to modulate the height of the induced supply glitch. Additionally, a glitch enable control is used to send narrow pulses to enable/disable these NMOSs to induce supply glitch with varying height and width (glitch profile depends on width of narrow pulse and on-chip decoupling capacitor). The clock for the test-chip is generated internally using a free-running VCO. The AES can operate in the standalone mode with a fixed frequency clock generated from the VCO. The AES can also operate in a protected

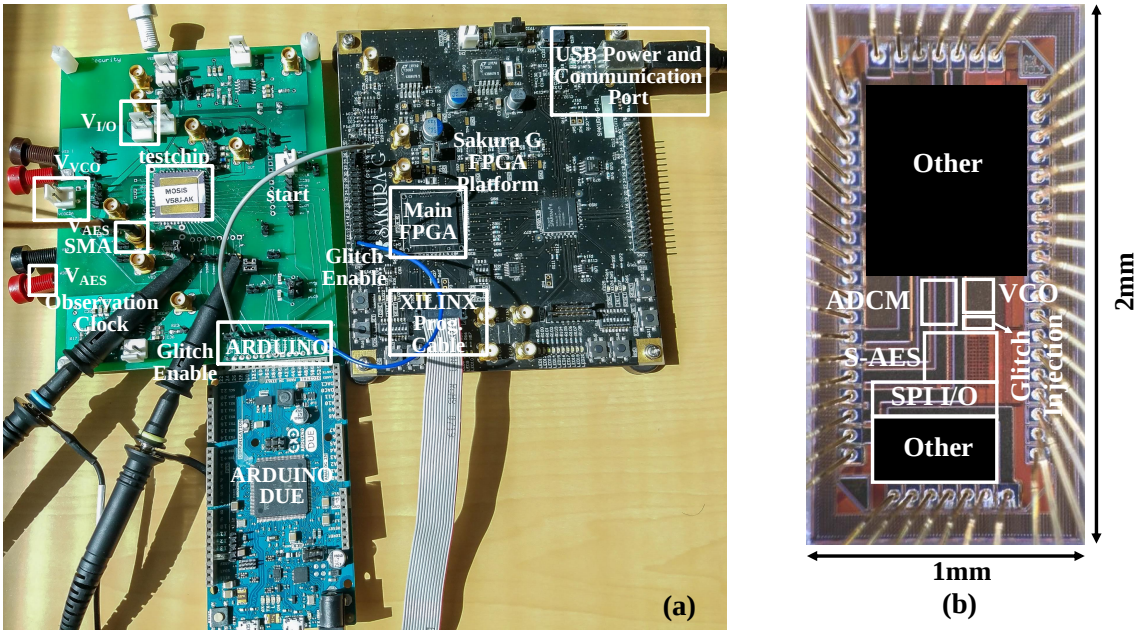


Figure 6.3: (a) Measurement setup with testchip and PCB integrated with Sakura-G FPGA platform and Arduino Due (b) testchip with relevant blocks marked for FIA experiments.

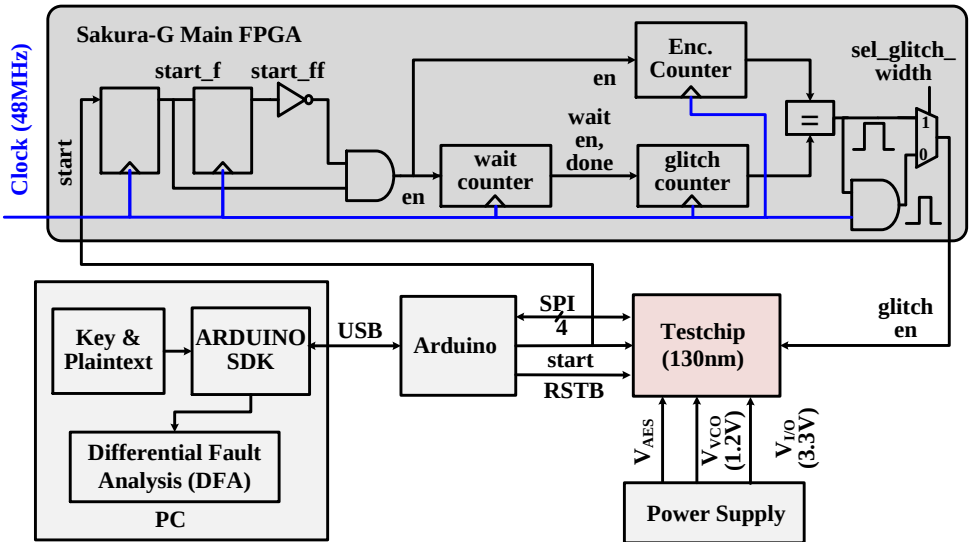


Figure 6.4: Measurement setup for fault injection- Sakura-G platform integrated with testchip to generate programmable glitch enable signal once every encryption.

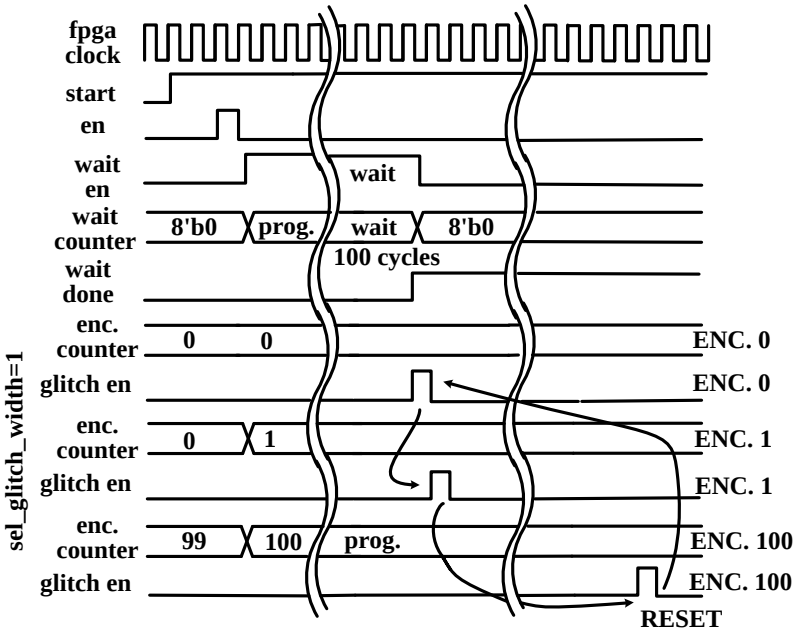


Figure 6.5: timing diagram for glitch enable generation with respect to AES encryption.

mode, where the AES clock comes from the ADCM circuit. In the protected mode, the ADCM circuit takes the VCO clock as the input and generates the AES clock as the output [Fig. 6.6].

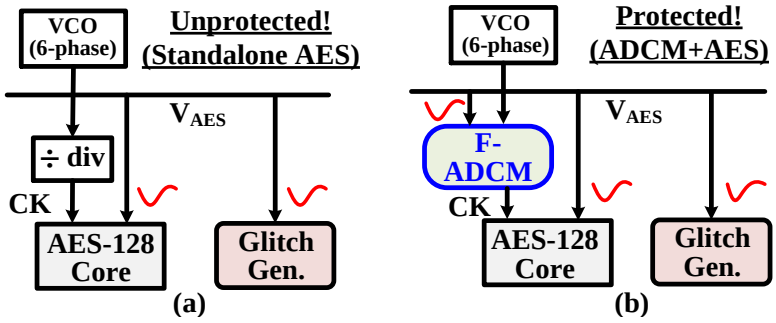


Figure 6.6: (a) Unprotected standalone AES and (b) AES protected with on-chip ADCM circuit are analyzed with respect to FIA.

Table 6.1: Summary of testchip with respect to S-AES, ADCM, VCO circuits.

S-AES Core	Area	320µm×360µm (6592 gates)
	Perf.	Latency: 502 cycles, Throughput: 28.1Mbps @1V, 110MHz
	Op. Range	0.58V (9.6MHz) - 1.25V (169.6MHz)
	Power	3.9mW @110MHz, 1V
ADCM	Area	100µm×145µm (1451 gates)
	Power	129µW @600MHz input, 110MHz output, 1V
	Freq. (VCO)	600MHz
	Op. Range	0.58V-1.25V @600MHz VCO clock
VCO	Freq. Range	93MHz - 600MHz
	V_{CTRL}	0 – 0.56V

6.3 Measured Results

6.3.1 Fault Injection and Analysis for Standalone AES

Fault Injection

To inject glitches in a controllable fashion, the testchip is supplied glitch enable signal from Sakura-G based FPGA board. The FPGA chip runs at 48MHz with 67% duty cycle. Glitch widths of 21ns/14ns are generated using full and high pulse period for the clock [Fig. 6.4]. With the assumption that we only have approximate information about S-AES rounds of operations, faults are injected towards the last few rounds only. The start signal used to start AES encryption is also used by the FPGA chip to generate glitch enable signal approximately in the proximity to the target rounds. In our experiments, to ensure

Table 6.2: Summary of testchip with respect to S-AES, ADCM, VCO circuits.

Glitch Level	Glitch Width=T_{FPGA_CLK}(21ns)					Glitch Width=T_{FPGA_CLKP}(14ns)				
	ΔV (mV)	Total Faults	16-Byte Faults			ΔV (mV)	Total Faults	16-Byte Faults		
			Total	Unique	Exploitable			Total	Unique	Exploitable
0001	111	0	0	0	0	90	0	0	0	0
0011	160	1188	1173	112	11	157	282	275	29	5
0100	207	2727	2622	731	43	215	1518	1415	206	28
0111	274	2965	2752	1430	52	267	2594	2450	653	60
1000	321	2966	2786	1599	28	320	2798	2624	1067	53
1111	384	2972	2796	1721	0	374	2958	2752	1329	28

the inclusion of target operation(s) for fault injection, the faults are injected over a longer duration (about 50% of total encryption duration - to approximately cover round 5 to round 10). When the encryption is started, a glitch counter circuit, after initial wait time is used to generate glitch enable at incremented clock cycles [Fig. 6.5]. Glitch counter circuit is reset after a programmable duration and whole process restarts. The wait, encryption (enc.) and glitch counters are reconfigured to inject faults at different AES clock frequencies (F_{AES}). Since the AES clock and FPGA clock are asynchronous, the timing of fault injection with respect to AES clock is random during each iteration of glitch counter. Also, since width of the glitch enable signal is larger than the AES clock period, the supply glitch may affect multiple bytes during AES operation.

Fault Model Selection

Since the faults are injected in a random fashion without accurate information/control on timing of the faults, the faulty ciphertexts will consist of both exploitable and unexploitable faults. To reduce the DFA time and computation complexity, we chose fault model proposed by Piret and Quisquater [89] for AES which is based on single-byte fault injection between MixColumn operation of round 7 and 8 and requires only 2 faulty ciphertexts to find correct key.

Fault Characterization and Analysis

Supply glitches are injected with different width (14ns and 21ns, controlled with glitch enable generation circuit on FPGA chip) and different height (90mV to 384mV with several intermediate levels, controlled with glitch_lvl signal) at nominal operating conditions (V_{AES}=1V and F_{AES}=110MHz). Fig. 6.7 and Fig. 6.8(a) show measured glitch height and width for few cases. Under large glitch, the level shifter between V_{AES} and VI/O cannot support high speed, therefore, observed clock waveform is distorted. Table 6.2 summarizes all the faults that are injected out of total 10,000 encryptions. Total number of faults increase with increased glitch width/height. Most of the faults injected are all (16) byte faults indicating a single-byte fault is induced before round 8 MixColumn or multi-byte faults are injected. It is observed that at smaller drop in supply voltage, the unique 16-byte faults are less compared to higher drop where most of the 16-byte faults injected are unique. For the fault attack, all unique 16-byte faults are filtered out and 2 faulty ciphertexts are randomly chosen for DFA until the key is recovered. The number of exploitable faults injected increase initially with increasing drop in supply voltage as more unique faults are injected, however as drop is increased further, exploitable faults decrease, mainly due to multi-byte faults injected with higher drop. At highest drop (384mV), none of the faulty ciphertexts

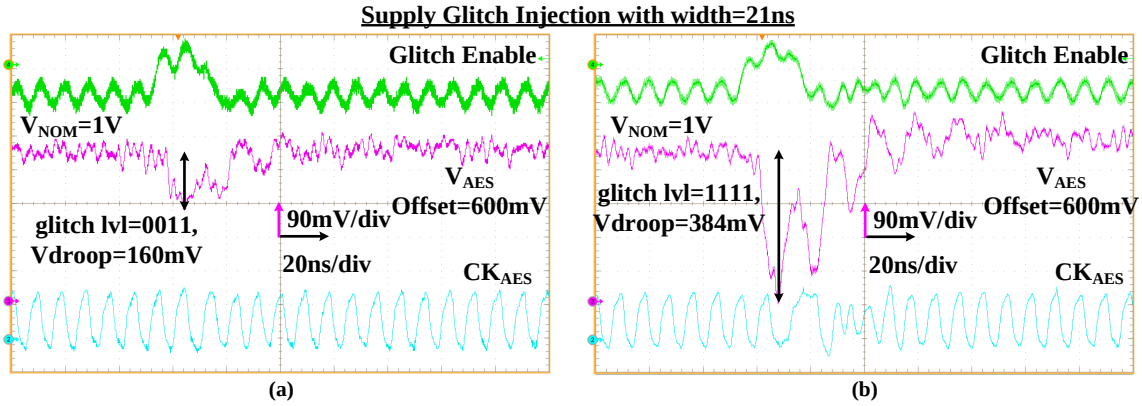


Figure 6.7: Glitch injection under nominal conditions (V_{AES}=1V, F_{AES}=110MHz) with programmable glitch height and width: (a) glitch level=0011, width=21ns, (b) glitch level=1111, width=21ns.

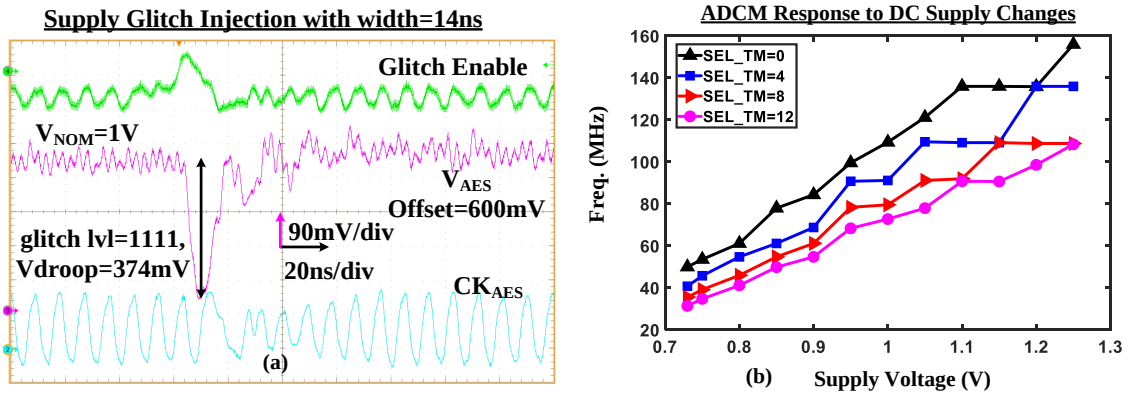


Figure 6.8: (a) Glitch injection under nominal conditions (V_{AES}=1V, F_{AES}=110MHz) with programmable glitch height and width: glitch level=0011, width=21ns and (b) Characterization of ADCM for DC supply voltage ranging from 0.72-1.25V.

were exploitable for a glitch width of 21ns. However, for same drop but 14ns glitch width, 28 exploitable faults were injected. The experiment indicates the importance of controlling glitch height and width, even when we inject glitches randomly during the encryption.

6.3.2 Fault Mitigation with ADCM (Protected AES Mode)

Supply Glitch at V_{AES}

In presence of supply drops, GM inside ADCM modulates CKG to prevent timing failures. Since in our design, GM is in proximity to S-AES, it can modulate the clock even in presence of local supply noise, therefore, LM doesnt play a big role. Fig. 6.9 (a) & (b) show operation of ADCM under highest glitch level (1111) at 1V and 0.72V. ADCM generates rising clock edges only when entire critical path is traversed under supply glitch (the output clock period is significantly increased at higher glitch levels). No faults could be injected at nominal operating conditions even after 10 million encryptions under all glitch profiles (width and level). However, when power supply is decreased to 0.8V and 0.72V, faults could be injected (1 fault @0.8V and 168758 faults @0.72V, though only 1 unique fault which is same at both supply conditions) even when ADCM is on. This could be caused by slight mismatch between critical path replicas and actual critical path circuit at low supply voltages or a very different path may be critical, not the one implemented with critical path

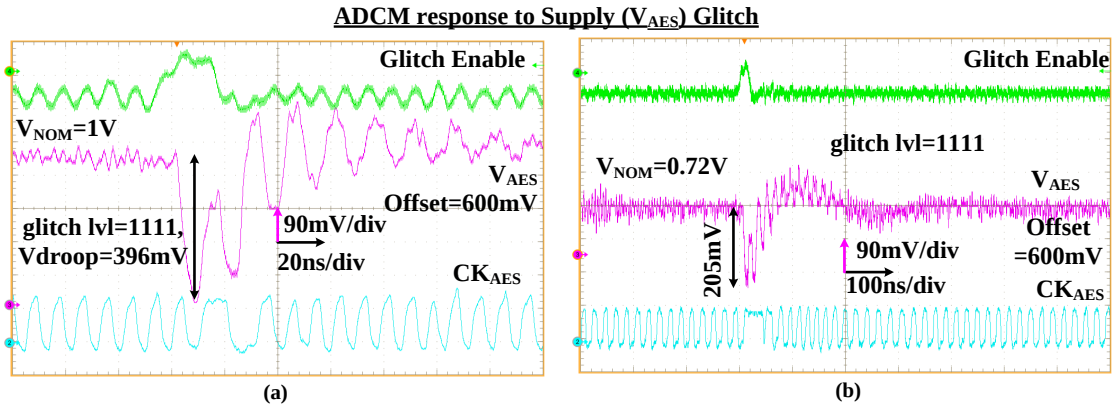


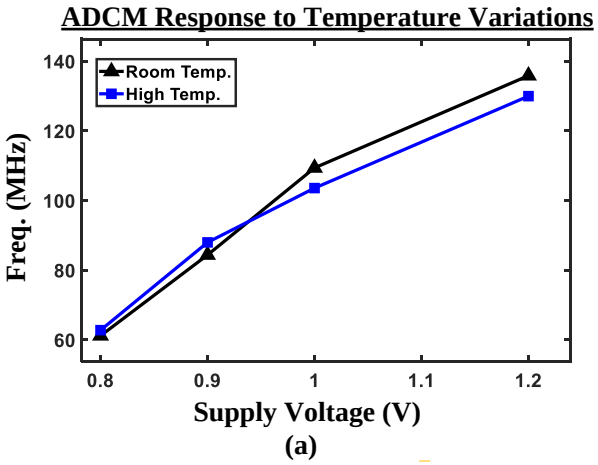
Figure 6.9: ADCM responds to supply glitches: (a) at nominal conditions (V_{AES}=1V, F_{AES}=110MHz) with the highest glitch level and (b) at V_{AES}=0.72V with the highest glitch level.

replicas as digital gates have very different behavior under extreme levels of supply noise which is not observed with simulation/STA.

To mitigate these faults, timing margin is added with the help of programmable trimmer inside GM (trimmer 0, configurable from 0-31 in increments of 1) with SEL_TM=2. With additional timing margin (SEL_TM=2), no faults could be injected at 0.8V/0.72V. Fig. 6.8(b) shows ADCM output clock freq. characterized with DC changes in supply voltage (0.72V-1.25V) for a few SEL_TM settings. When the supply voltage is further reduced, the level shifter [Fig. 6.1] between core (V_{AES}) and I/O (3.3V) domains fails and internal clock can no longer be observed. However, AES correctly operates up to 0.58V. We couldnt inject any faults at 0.58V even with highest glitch level. When supply is further reduced, ADCM and AES circuits completely fail and generate 16-byte unexploitable faults.

Temperature Variations

The delay of CMOS gates changes under temperature variations. To study the effect of temperature on injected faults and ADCM generated output clock frequency, testchip was subjected to hot air flow for 30 seconds with a 120V/300W heat gun from about 3cm. Fig. 6.10(a) shows the response of ADCM at room temperature and high temperature. Inverse temperature dependence is observed in the output clock frequency. Therefore,



Fault Injection with Temperature Variations @V_{AES}=1V, F_{AES}=110MHz

	# of Faults (Total, Unique, Exploitable)	
	Room Temperature	**High Temperature**
Standalone AES	**1,1,0**	**3376,1,0**
ADCM + AES	**0,0,0**	**0,0,0**

(b)

Figure 6.10: (a) effect of increased temperature on ADCM output clock freq., and (b) more faults are injected at high temperature at nominal conditions (V_{AES}=1V, F_{AES}=110MHz) however with ADCM turned ON, all faults are prevented.

FIA becomes critical at higher voltages under overheating. At nominal operating conditions (F_{AES}=110MHz, V_{AES}=1V), only one fault could be injected at room temperature after 100K encryptions while number of faults increase to 3376 at high temperature [Fig. 6.10(b)]. A skilled adversary can control the testchip temperature to induce temperature dependent faults during the last few rounds for FIA. With ADCM turned on, no faults are injected with 100K encryptions at room temperature or high temperature.

Supply Glitch at V_{VCO}

Since an adversary doesnt have access to internal clock when ADCM is ON, he/she may still alter VCO supply clock to modify the operation of ADCM itself. We shorted VCO supply (VVCO) with V_{AES} to investigate the effect of supply glitch on VCO and there fore ADCM. Under nominal conditions, we couldnt inject any faults however at VVCO=0.9V [Fig. 6.11(a)], we were able to inject same fault as observed for V_{AES}=0.72V in previous section. This fault goes away for SEL_TM=2. When VVCO is further reduced, both VCO and ADCM operate reliably at reduced DC supply however under supply glitch, it is no longer operational [Fig. 6.11(b)].

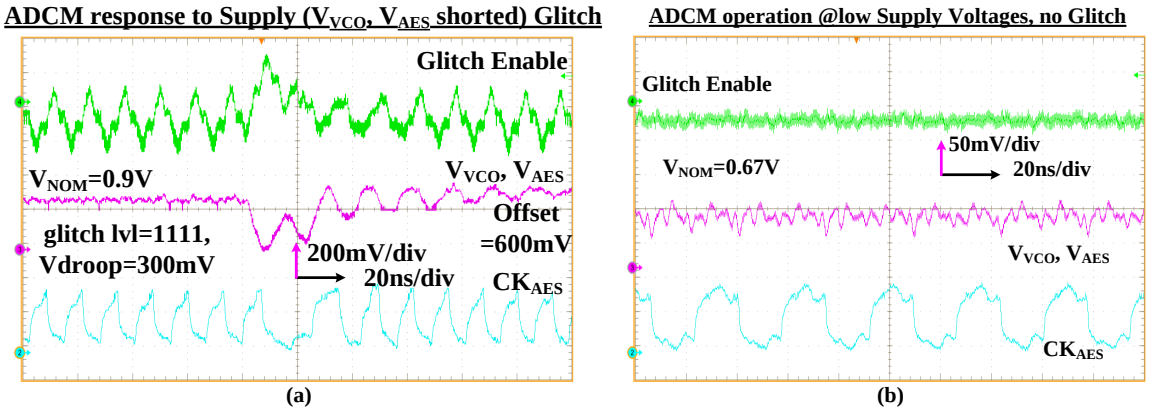


Figure 6.11: (a) effect of glitch on VCO supply voltage when V_{AES} and VVCO are shorted, ADCM still operates reliably under glitches and (b) Impact of reducing V_{AES}, VVCO (shorted) to very low levels.

6.3.3 Discussion

Traditionally error-resilient circuits have been designed to tolerate and correct for timing errors under small supply glitch to increase performance. Exploiting these timing error detection/correction and prevention (ADCM) circuits to mitigate fault attack is an interesting research direction as an adversary will try all possible methods to make the circuit fail even with abnormal operating conditions, e.g. high supply glitches. Additionally, the error-resilient circuits may themselves fail giving rise to a possible path to inject faults in the cryptographic hardware. We observed the need to build timing margin to account for any layout mismatches or in case some other path is activated under certain conditions. Design flow in [139] can be used to minimize these mismatches. Additionally, parasitics of on-chip power delivery network will create small mismatches in the exact timing of injected glitch at ADCM and AES. A proficient adversary may be able to exploit these differences to inject faults. However, for a large design, it is recommended to have distributed local modulator circuits to respond to local supply noise. Additionally, ADCM cannot prevent timing errors due to hold failures [95]. With large +ve spikes in supply voltage, short paths in S-AES (primarily related to control/finite state machines) can be activated. However, a guardband can be built into the design to tackle hold issues at small area and power over-

heads without any impact on performance. Moreover, since proposed ADCM generated output clock period is a multiple of source clock period, input data-dependent fluctuations in critical path delay (may lead to an unintentional timing side channel) are only minimally reflected in the generated clock.

Compared to other error-resilient architectures, ADCM prevents timing errors from occurring while other techniques, such as Razor [72], may completely stall the pipeline resulting in denial-of-service attacks. Additionally, unlike Razor which requires modifying the sequential elements, ADCM doesnt require any modification in the underlying hardware and therefore has very small overheads (12.5% area and 3.3% power Table 1). Finally, ADCM doesnt require any complex glitch detection circuits like in [43].

6.4 Summary

This chapter demonstrated that a ADCM circuit, normally designed to increase variation tolerance, can also prevent supply glitch and temperature variations-based fault injection attacks. Measurement results from a 130nm CMOS test-chip showed successful DFA attack on a standalone S-AES digital core with externally controlled fault injections and programmable glitch width and height. However, when ADCM is turned on to provide clock to S-AES, no fault could be injected even after 10 million encryptions under wide range of operating conditions. ADCM can mitigate both supply glitch and temperature variation induced faults and incurs only 12.5% area and 3.3% power overheads and improves performance under supply transient noise.

CHAPTER 7

LIGHTWEIGHT SCA COUNTERMEASURES UTILIZING INTEGRATED DIGITAL LDO

The recent trends in utilizing on-chip integrated voltage regulators (VRs) to provide SCA protection show that they can help in two ways - 1) by isolating the measurement node of the IC from the local supply node of the encryption engine and 2) by inducing frequency dependent transformations that help in suppressing the information leakage. Authors in [46, 47, 50, 129, 140, 141] presented several countermeasures based on switching DC-DC regulators (both inductive and switched capacitor) against P-SCA attacks. Authors in [100, 135] demonstrated that integrated inductive voltage regulator (IVR) can also be used to protect against EM-SCA attacks due to constant switching of IVR power-stage and inductor current in the proximity of the encryption engine. In Chapter 5, we saw that IVR when integrated with ADCM circuit can also be used to randomize EM signatures generated from AES and therefore provide SCA resistance. However, due to requirement of large passives (L, C) and high complexity of these regulators, usually the same regulator is shared across the entire processor and encryption hardware, therefore any randomization scheme employed to further enhance the SCA resistance [46] affects the performance of the entire system [Fig. 7.1]. Authors in [81, 83, 84] have demonstrated P-SCA resistance offered by both digital and analog LDO regulators with simulation studies. Digital LDOs do not require any inductor, are simpler to design and are scalable across process nodes and therefore are very suitable for ultra fine-grained power management and point of load regulation [40, 41].

This chapter presents the 130nm CMOS testchip designed to experimentally demonstrate improved power and EM SCA resistance of standard (unprotected) 128-bit AES and SIMON cores via an on-die security-aware all-digital series LDO regulator [Fig. 7.1]. The

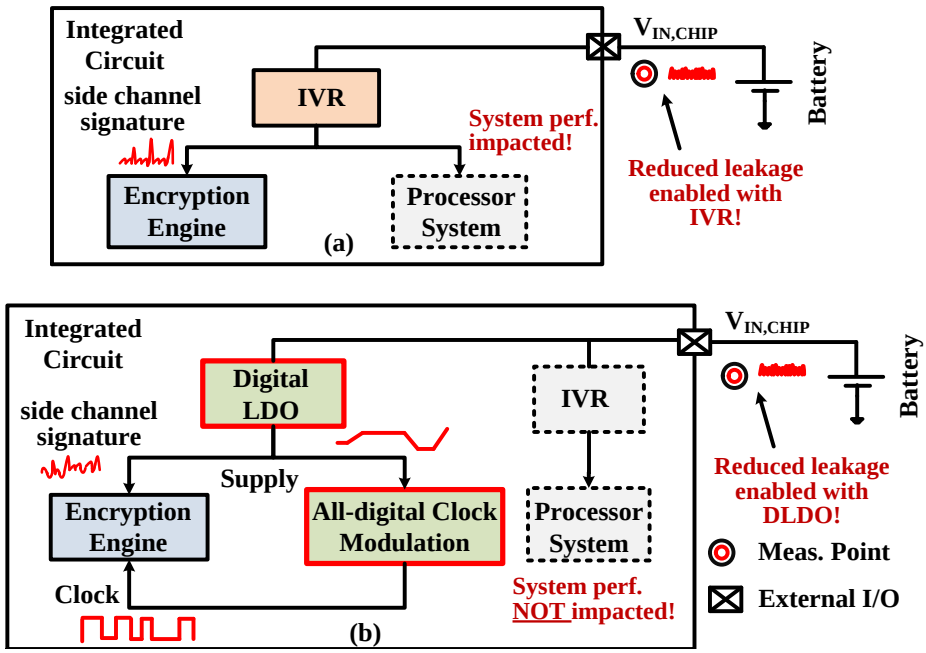


Figure 7.1: Utilizing integrated voltage regulators as SCA countermeasures, (a) limitations of switching DC-DC converter based SCA protection schemes and (b) proposed on-die digital LDO integrated with ADCM circuit for simultaneous supply and clock modulation to improve SCA resistance.

testchip consists of proposed 250MHz DLDO with 2.3nF output capacitor powering two 128b AES cores (parallel AES: P-AES and serial AES: S-AES) [142] and a 128b SIMON core along with 2 randomization circuits (SNI and R-VREF) [Fig. 7.2].

The rest of the chapter is organized as follows. Section 7.1 presents system architecture and perform model analysis for the proposed DLDO; Section 7.2 presents SNI & R-VREF circuit techniques that are proposed to further enhance SCA resistance; Section 7.3 presents simulation studies for the impact of digital LDO on SCA leakage from encryption engines; Section 7.4 discusses measurement setup and postprocessing methods; Section 7.5 present the measured results with respect to P-/EM-SCA; and Section 7.6 summarizes the chapter.

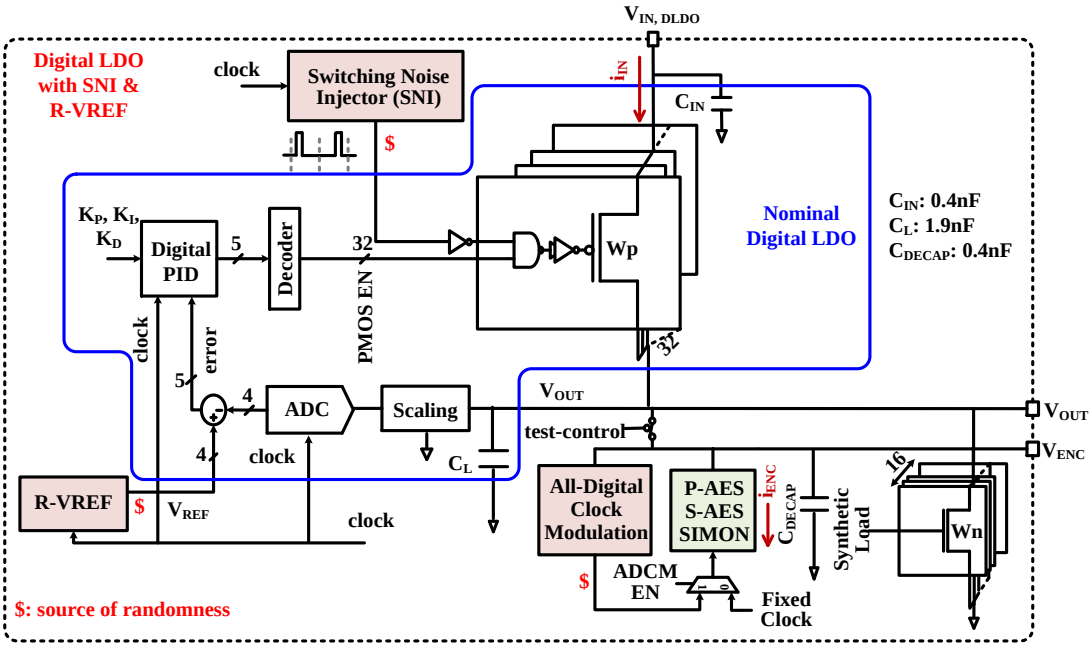


Figure 7.2: System architecture consisting of nominal DLDO, AES and SIMON cores, proposed SNI, R-VREF R-VREF & ADCM circuits.

7.1 System Architecture

7.1.1 Design of Encryption Engines

Two different encryption algorithms (128-bit AES and 128-bit SIMON) are implemented on the testchip. For AES algorithm, two cores, one with 128-bit parallel (P-AES) datapath and other with 8-bit serial (S-AES) datapath while for SIMON algorithm, a bit-serial (1b) datapath has been implemented. The architecture for these datapaths has been presented in Chapter 3.

7.1.2 Design of Digital LDO

A fully-synthesizable digital LDO is integrated on-chip to provide currents and regulate supply voltage to the encryption cores. The proposed digital LDO consists of a power-stage with 32-bit equally sized PMOS elements, a programmable resistor-divider for scaling the output voltage, a 4-bit delay-line based analog-to-digital converter (ADC) and a digital proportional-integral-derivative (DPID) controller. A 5-to-32 decoder decodes 5-bit binary

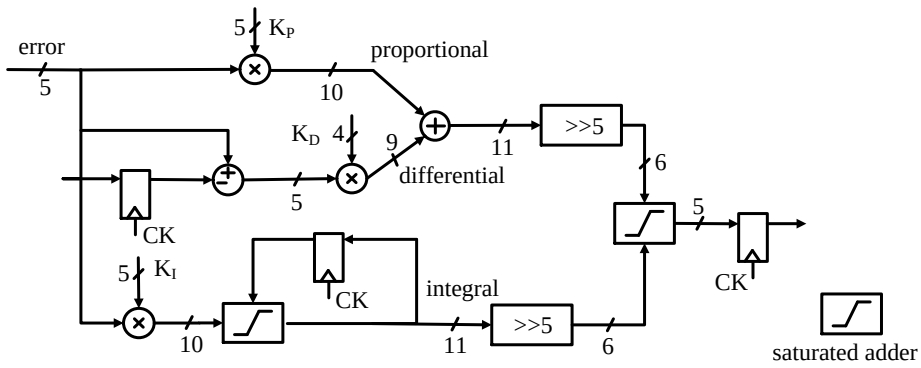


Figure 7.3: Digital implementation of proportional-integral-derivative (PID) compensator in parallel form.

output of DPID controller into 32-bit thermometer code to control PMOS devices in the power-stage. An output capacitor of 1.9nF is integrated on-chip using metal-insulator-metal (MIM) technology. DPID controller, a type-III compensator with 2 zeros and 2 poles, is implemented in its parallel form [Fig. 7.3]. It takes 5-bit error as an input and generates 5-bit compensated output based on 5-bit proportional (K_P), 5-bit integral (K_I) and 4-bit derivative (K_D) gains. Both ADC and DPID controller datapaths are optimized to run at 250MHz on-chip voltage-controlled-oscillator (VCO) generated clock.

7.1.3 Transformations via Digital LDO

Measured supply current at the input supply ($V_{IN,DLDO}$) of the chip is a transformed version of the internal on-die supply current of the encryption engine measured at local supply node (V_{ENC}). This section presents theoretical analysis for transformations that encryption current undergoes through digital LDO before it is measured at the input supply node.

For small-signal modeling, all the blocks including sample and hold, delay-line ADC, PID compensator, zero-order-hold (ZOH), power-stage and the output load are modeled as below:

ADC is modeled using ADC gain and 1-cycle delay:

$$H_{ADC}(z) = \frac{1}{v_{LSB}} \times z^{-1} \tag{7.1}$$

where v_{LSB} is the analog voltage change for 1 LSB (least-significant-bit) difference in the digitized ADC output.

The z-domain transfer function for the type-III compensator is given as below:

$$G_C(z) = \left[k_p + \frac{k_i}{1 - z^{-1}} + k_d(1 - z^{-1})\right] z^{-1} \tag{7.2}$$

where k_p, k_i and k_d are proportional, integral and derivative gains respectively. The PID compensator transfer function has three poles, two of those at $z = 0$ (one pole due to 1-cycle delay) and another pole at $z = 1$, two zeros whose locations are determined by the compenstor gains $\{k_p, k_i, k_d\}$. Fig. 7.3 describes the digital implementation of compensator with fixed/reduced precision arithmetic. Since the output of PID compensator is registered, a single cycle delay (z^{-1}) is incorporated in z-domain transfer function. Effective gains for the PID compensator can be represented as below:

$$k_p = \frac{K_P[4:0]}{32},\ k_i = \frac{K_I[4:0]}{32},\ k_d = \frac{K_D[3:0]}{32} \tag{7.3}$$

The transfer function for the power-stage in z-domain can be represented as follows [63]:

$$P(z) = \frac{K_{DC}(1 - e^{-w_L T s})}{(z - e^{-w_L T s})} \tag{7.4}$$

where $K_{DC} = I_{PMOS} \times R_P \| R_L$, I_{PMOS} is the current capacity of a single PMOS unit, $\omega_L = \frac{1}{(R_P || R_L) C_L}$ is the load pole and $T_s = \frac{1}{F_s}$ is the sampling period. For steady-state stability/ripple analysis, the PMOS array is modeled as an effective resistance R_P but for transient simulation, PMOS devices are modeled using PMOS current equations (large-signal) in triode and saturation regions. In steady-state, PMOS is always assumed to be in triode region with a constant PMOS device resistance. Effective resistance of power-stage is determined by dropout voltage (V_{DO}) and load current (I_L, $R_P = \frac{V_{DO}}{I_L}$ in steady state).

Open-loop/closed-loop transfer function for the DLDO system can be derived with z-

domain transfer functions for the individual blocks:

$$H_{OL}(z) = z^{-2}.\frac{K_{OL}(z - z_{PI})(z - z_{PD})}{(z-1)(z - e^{-w_L Ts})} \tag{7.5}$$

where K_{OL} is the DC gain for the open-loop DLDO system and z_{PI}, z_{PD} are two zeros added by the PID compensator.

$$H_{CL}(z) = \frac{H_{OL}(z)}{1 + H_{OL}(z)} \tag{7.6}$$

The DLDO power stage acts as a low-pass filter with bandwidth dictated by the equivalent resistance of the power stage and output capacitor, thereby attenuating the high freq. current signatures. The DLDO control loop induces freq.-dependent small signal and large signal perturbations dictated by the loop delay and zero/pole locations. Any current fluctuations in the encryption engine has two paths to propagate to the input of the DLDO 1) a direct path through the power-stage to the DLDO input or 2) through the feedback path including the ADC, digital PID compensator and the power-stage to the input of DLDO. Both of these paths introduce freq. dependent large and small signal transformations in the encryption/load current. The small signal perturbation at the encryption current/load current of the DLDO goes through a freq. dependent transformation before it appears at

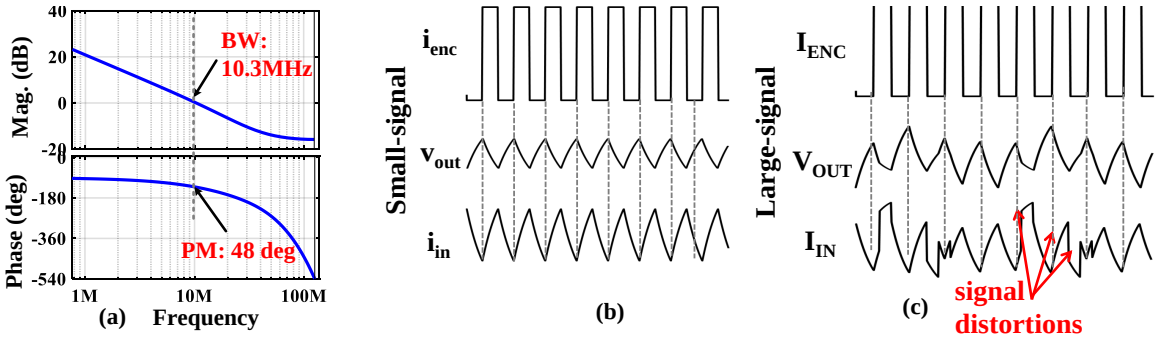


Figure 7.4: DLDO model analysis and transformations. (a) Bode plot for the open loop DLDO under nominal operating conditions and at 31mA base current, (b) small signal attenuation and (c) large signal amplitude distortions.

the input current. Current transformation from encryption current to input current can be modeled using a transfer function for the DLDO as discussed above in Eq. 7.5. The load pole , poles and zeros added with PID compensator and ADC as well as open-loop DC gain of the system determine the small signal transformations and the bandwidth of the DLDO system. Due to limited bandwidth of the closed-loop DLDO system (open loop bode plot in Fig. 7.4(a) shows a bandwidth of 10.3MHz), high freq. components of encryption current are significantly attenuated. In addition to small-signal transformations, under large and sudden variations in load current, nonlinear characteristics of the PMOS devices and the control loop must be taken into considerations to determine the large signal transformations. Large signal transformations lead to information loss which can be attributed to limited sampling of the output voltage, quantization losses through the ADC, controller and power-stage. Fig. 7.4(b) and (c) show attenuation of high-freq. signatures due to small-signal and signal distortions due to large-signal characteristics of the DLDO closed loop.

7.2 Proposed Circuit Techniques

Two circuit techniques proposed to improve the SCA resistance in addition to what is offered by the nominal DLDO are described below:

7.2.1 Switching Noise Injection (SNI)

One major leakage path for DLDO is through the enabled PMOS devices which are always "ON" and connect output V_{ENC} directly to the input $V_{IN,DLDO}$. Even though this path acts as a low pass filter (LPF) with cutoff freq. dependent on the effective resistance ($R_P \| R_L$) and effective capacitance (C_L) at the output node, low-freq. signals in the encryption current directly propagate to $V_{IN,DLDO}$. To prevent leakage via this path, we propose SNI circuit which disconnects V_{ENC} from $V_{IN,DLDO}$ for a very small fraction of the DLDO clock cycle [Fig. 7.5(a)]. SNI circuit consists of 9 pulse generators. Each pulse generator receives 9

positive (p) and 9 negative (n) phases from the 9-phase differential delay cell based VCO and generates a pulse (pulse out) with programmable width every DLDO clock cycle. All the 9 pulses (pulse0, pulse1, ..., pulse8) are spread across the DLDO clock cycle and the output of a free-running linear feedback shift register (LFSR, LFSR1) selects one of these 9 pulses every DLDO clock cycle, thus ensuring pseudo-random location of generated pulse out signal. The width of these pulses can be programmed to be one of 3 possible widths based on user specified settings or using an on-chip LFSR (LFSR2) [Fig. 7.5(b)]. When SNI is enabled, during the high level of the SNI pulse, DLDO is disconnected, the output voltage drops significantly with total drop determined by the pulse width as well as the size of load capacitor (C_L). When SNI pulse is de-asserted, DLDO becomes operational, however, due to large drop in the output voltage, feedback loop tries to compensate for the large error which results in the overshoot [Fig. 7.5(c)]. Since an SNI pulse is generated every DLDO clock cycle, it results in consistent spikes in the supply voltage. Additionally, due to pseudo-random nature of the SNI pulse, the spikes are also pseudo-random, therefore achieving randomization in the power supply for the encryption cores. However, due to large spikes in the supply, to ensure correct operation, we propose integrating clock modulators to tolerate additional supply noise.

7.2.2 All-digital Clock Modulation (ADCM) Circuit

ADCM circuit [100] responds to any DC shift/transient noise in supply voltage at cycle-by-cycle speed. ADCM utilizes critical path replica (CPR) based global modulator (GM) and local modulator (LM) to achieve this. GM responds to DC shift and global noise while LM ensures correct operation under local supply noise. GM runs at very high VCO clock freq. ($\approx$ 600MHz) and generates a clock with clock period multiples of VCO clock period tracking the critical path delay. LM takes output of GM as input and stretches the clock edges in duty modulation or skips clock edges in clock gating mode to ensure correct clock edges are generated. The CPR is implemented for P-AES which has the worst case path

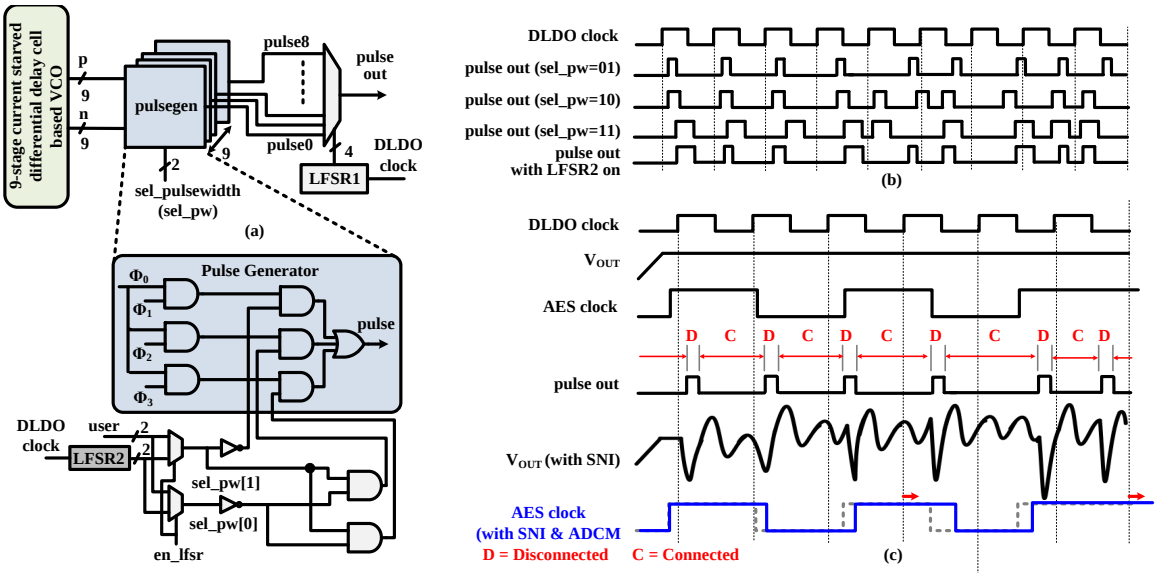


Figure 7.5: Block diagram for (a) proposed SNI circuit, (b) circuit operation, and (c) supply and clock randomization achieved with SNI and ADCM.

of all 3 encryption cores. With ADCM enabled, temporal noise is added due to pseudo-random nature of shifts added in the clock edges. The amount of temporal noise depends on the average voltage noise added during each encryption clock cycle [Fig. 7.5(c)] and helps in SCA protection.

7.2.3 Random VREF Generator (R-VREF)

We propose to further scramble the power/EM signatures using simultaneous supply and clock modulation using DLDO and ADCM circuit. Random VREF generator (R-VREF) circuit randomizes the reference word input to the DLDO [Fig. 7.6(a)]. To achieve this, 16

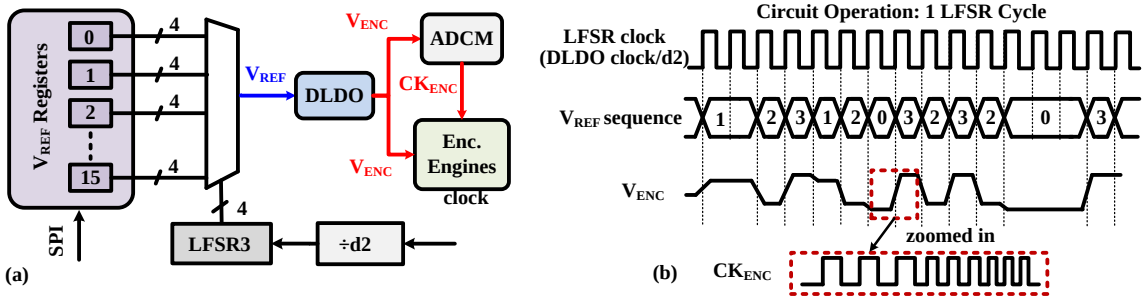


Figure 7.6: Block diagram for (a) proposed R-VREF circuit and (b) circuit operation.

VREF words (each 4-bit) are loaded on 16 on-chip 4-bit registers. A 4-bit full-length LFSR (LFSR3) can select any of these words based on its output. LFSR clock which controls the speed of VREF update is derived from the DLDO clock using a divider with division setting configurable to divide-by-1, 4, 16 or 64. Fig. 7.6(b) shows the circuit operation for the R-VREF. As reference word is updated with R-VREF generator, DLDO system responds and V_{ENC} tries to track these changes. V_{ENC} is also fed to the ADCM which generates correct clock edges under DC changes in supply as well as during transitions. Due to limited dynamic range of DLDO, only 4 different values for VREF could be programmed.

7.3 Simulation Study for Impact of Digital LDO on Side Channel Leakage from Encryption Engines

In this section, we model the digital LDO as discussed in Section 4.1.2 and Section 4.1.3 and analyze the impact of digital LDO on side channel leakage from P-AES with respect to correlation power analysis (CPA) and signal-to-noise ratio (SNR). We vary various parameters, such as ADC resolution (Q_{ADC}) and sampling frequency (F_s), PID compensator gains (k_P, k_I, k_D) and sampling speed for the controller (F_s), and analyze their impact on SCA.

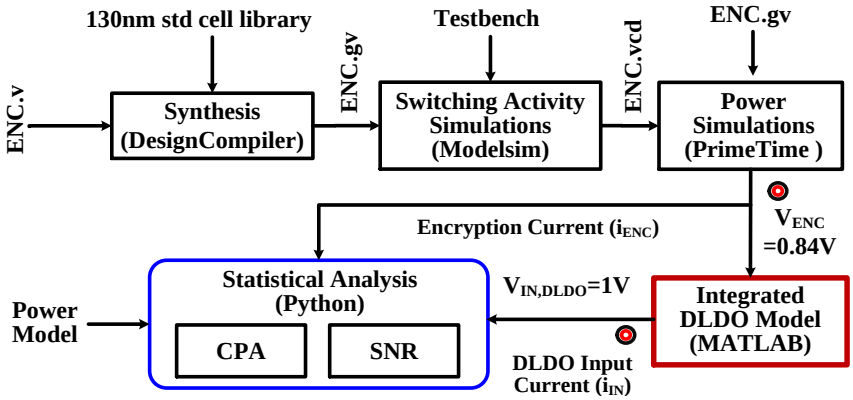


Figure 7.7: Simulation framework for integrated digital LDO and encryption core.

7.3.1 Simulation Framework

Fig. 7.7 shows the integrated framework combining encryption engines and digital LDO. The input verilog for the encryption core is synthesized using Synopsys DesignCompiler (DC) tool to generate gate level netlist using GlobalFoundary's 130nm standard (std) cell library. The gate level netlist is functionally simulated using an input testbench to generate switching activity values for all the internal nodes during an encryption. Power simulations are performed on the gate level netlist with parasitics (SDF) and switching activity file as inputs using Synopsys PrimeTime PX to obtain power/current consumption profile as a function of time. This current consumption profile (encryption current, I_{ENC}) is used as a load current for the the digital LDO to generate the input current profile at the input of DLDO (I_{IN}). The encryption current profile is sampled at the rate of 1ps per sample (same as the precision for the Modelsim functional simulations).

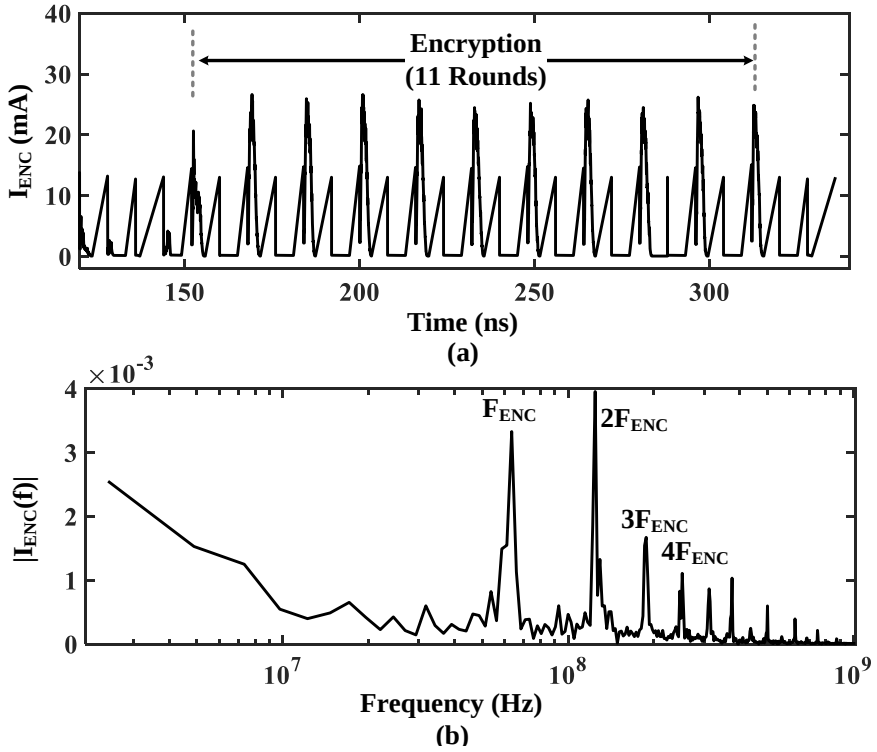


Figure 7.8: (a) Simulated current waveform for one P-AES encryption and (b) spectral content shows major peak corresponding to encryption clock frequency (F_{ENC}) and its harmonics.

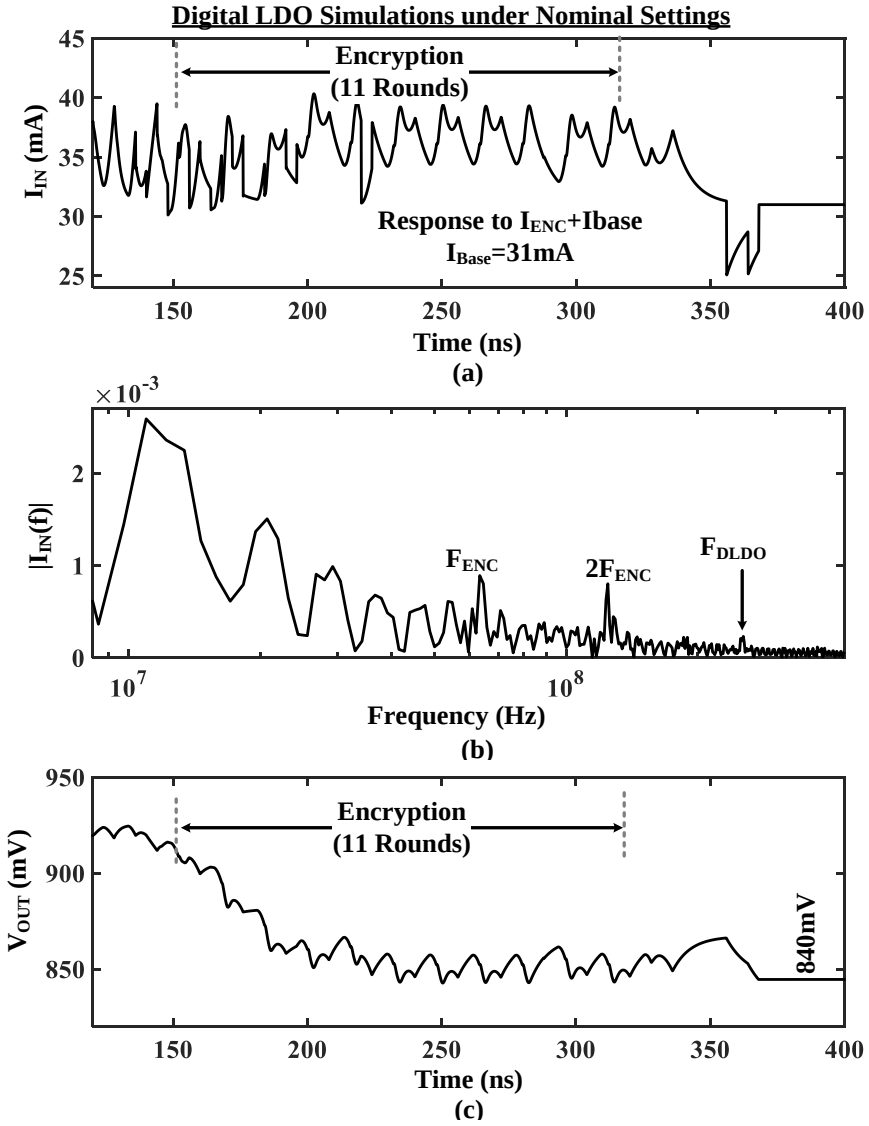


Figure 7.9: (a) Current profile at the input of DLDO (I_{IN}) in response to changes in the encryption current for one P-AES encryption, (b) spectral content shows major (but attenuated with respect to P-AES without DLDO) peak corresponding to encryption clock frequency (F_{ENC}), its harmonics and a small peak at the DLDO clock frequency (F_{DLDO}) and (c) output waveform (V_{OUT}) for the digital LDO under load changes due to encryption operation.

Fig. 7.8(a) shows the encryption current profile for 1 P-AES encryption running at 62.5MHz (F_{ENC}) encryption clock frequency. Large spikes are observed for each round of P-AES which is computed in one clock cycles. Additionally, slightly smaller spikes are also observed at both positive and negative clock edges. FFT of the encryption current shows a major peak at the encryption clock and its harmonics (2×, 3×, ...) [Fig. 7.8(b)]. The

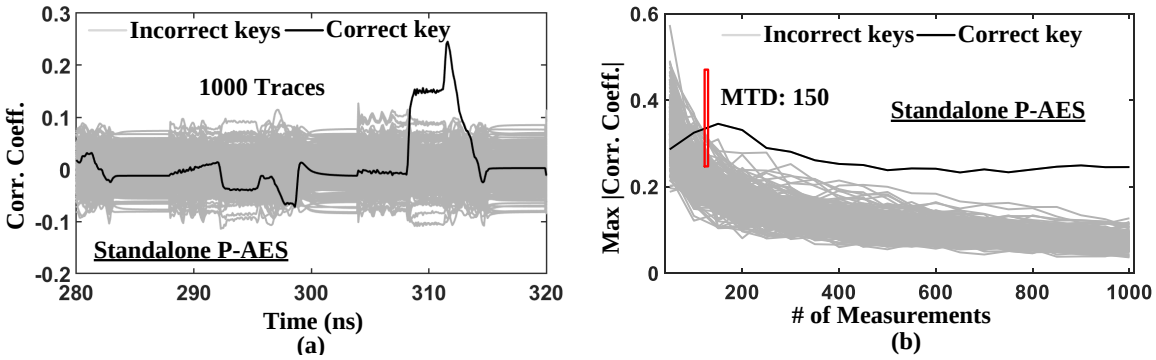


Figure 7.10: CPA attack results on the standalone P-AES core at local supply node (V_{ENC}) for subkey/byte 9: (a) correlation plot with 1000 simulations/traces and (b) MTD plot shows correct subkey 9 can be recovered with only 150 simulations/traces.

current profile at the input of DLDO is shown in Fig. 7.9 along with its FFT and profile for the output voltage (V_{OUT}). The high frequency signals in the encryption current are found to be significantly attenuated due to limited bandwidth of the DLDO under nominal operation conditions (10.3MHz, Table 7.2). The low-frequency spectrum is dominated by DLDO transient response characteristics. In addition to amplitude attenuation, significant amplitude distortions are observed in the input current (I_{IN}) due to frequency dependent delays added through the DLDO. A smaller peak corresponding to DLDO clock frequency (F_{DLDO} or F_s) is also observed in the FFT of I_{IN}.

7.3.2 SCA for Standalone P-AES

Both CPA and SNR analysis, as described in Chapter 3 (Section 3.2.1 and 3.2.2), are performed on the simulated encryption current for the P-AES encryption core in the time domain. A moving average with 1000 points (equivalent to 1ns) based filter is used to post-process and average out the noise (timing and amplitude). All the 16 subkeys for 128-bit P-AES key are correctly revealed with CPA attack and subkey 9 (out of subkeys 0 to 15) is found to be the highest leaking (minimum MTD) subkey. Fig. 7.10(a) shows the correlation coefficient plotted against time for 1000 simulations. The number of simulations/traces required to reveal the subkey 9 correctly is only 150 [Fig. 7.10(b)]. SNR for subkey 9 is computed with 1000 simulations. Table 7.2 shows that the SNR for standalone

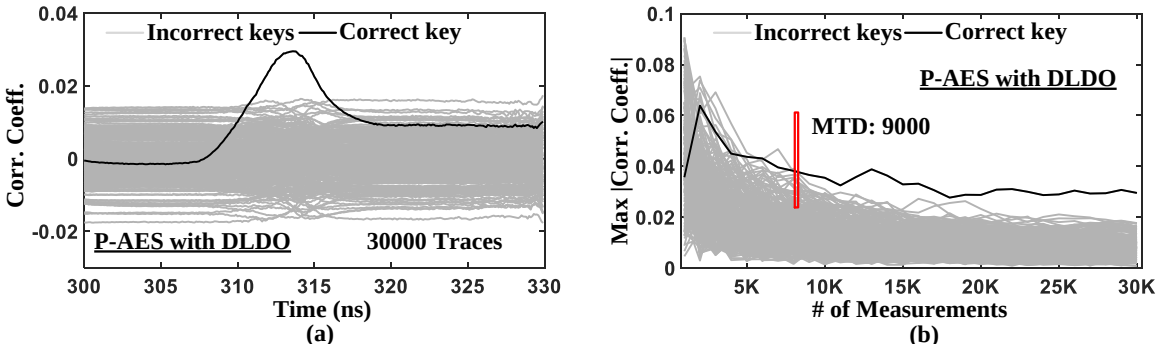


Figure 7.11: CPA attack results on the DLDO powered P-AES core at the input of DLDO ($V_{IN,DLDO}$) for subkey/byte 9: (a) correlation plot with 30000 simulations/traces and (b) MTD plot shows correct subkey 9 can be recovered with 9000 simulations/traces, indicating an increase of 60× with respect to standalone P-AES core.

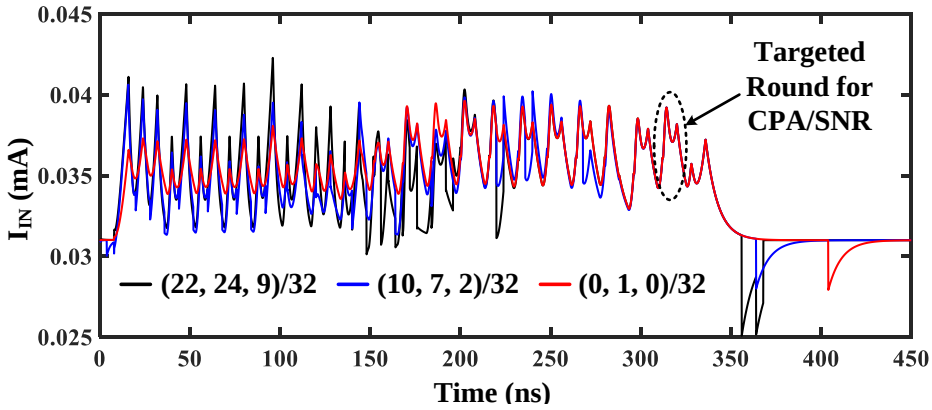


Figure 7.12: Effect of PID compensator gains on the DLDO transient response to the encryption current.

P-AES (without DLDO) is 0.178.

7.3.3 Impact of Digital LDO

For the DLDO powered P-AES core, the simulated current at the input of DLDO (I_{IN}) has attenuated and distorted signals leading to reduced SNR and increased difficulty in CPA attack. Correlation plot in Fig. 7.11(a) shows that subkey 9 for the P-AES core with DLDO can still be correctly recovered with 30000 simulations however MTD plot in Fig. 7.11(b) shows that 9000 simulations are required at the minimum indicating an increase of 60× with respect to just the P-AES core (without the DLDO). SNR analysis in Table 7.2 shows a degradation of 6.88× (0.1788 to 0.026) under nominal operating conditions and

Table 7.1: Configurations of Digital LDO analyzed with respect to their impact on SCA leakage for P-AES.

Standalone P-AES	Clock Freq.: 62.5MHz
Digital LDO	**Nominal:** F_s=250MHz; Q_{ADC}=25mV; PID Gains - $k_P=\frac{22}{32}$, $k_I=\frac{24}{32}$, $k_D=\frac{9}{32}$; V_{IN}=1V; V_{OUT}=0.84V; C_L=2.3nF; I_{Base}=31mA **Range of Controller Parameters:** F_s: 10MHz, 100MHz, 250MHz, 500MHz, 1GHz, 2GHz, 5GHz Q_{ADC}: 6.25mV, 12.5mV, 25mV, 50mV, 100mV PID Gains: $\{k_P, k_I, k_D\}=\frac{\{22,24,9\}}{32}, \frac{\{10,7,2\}}{32}, \frac{\{0,1,0\}}{32}$

controller settings.

Impact of Controller Parameter(s)

Next we analyze the impact of various controller parameters on the CPA attack results with respect to MTD and SNR values. CPA was performed with upto 32000 simulations while SNR was computed with 1000 simulations for all configurations as shown in Table 7.2. ADC resolution (Q_{ADC}) not only adds more quantization losses through ADC, it modifies

Table 7.2: Comparison of DLDO bandwidth and stability margins with SCA leakage for different values of controller parameter(s).

Design/Parameter	Controller Parameter(s)	Bandwidth (MHz)	Phase Margin (degrees)	CPA (MTD)	SNR (1000 traces)
Standalone P-AES	-	-	-	**150**	**0.179**
Nominal DLDO	Q_{ADC}=25mV, F_s=250MHz, k_P, k_I, k_D=(22, 24, 9)/32	**10.3**	**48**	**9000**	**0.026**
ADC Resolution (Q_{ADC}, mV)	**6.25**	**37.3**	**-39 (Unstable)**	**28000**	**0.0207**
	12.5	**17**	**19.2**	**>32000**	**0.016**
	50	**5.4**	**67**	**5000**	**0.119**
	100	**2.7**	**78.5**	**5000**	**0.119**
Sampling Freq. for both ADC & controller (F_s, MHz)	**10**	**0.46**	**63.5**	**20000**	**0.034**
	100	**4.5**	**58.8**	**9000**	**0.026**
	500	**17.7**	**37.2**	**9000**	**0.026**
	1000	**27.8**	**27.4**	**>32000**	**0.015**
	2000	**41.7**	**19.8**	**>32000**	**0.023**
	5000	**68.1**	**12.6**	**>32000**	**0.0335**
PID Gains (k_P, k_I, k_D)	**(10, 7, 2)/32**	**3.2**	**78.8**	**9000**	**0.026**
	(0, 1, 0)/32	**0.46**	**87.4**	**9000**	**0.026**

the open-loop DC gain of the feedback loop. A higher gain means higher bandwidth, however, a very high gain may lead to reduced phase margin and in some cases unstable loop. On the other side, a very poor ADC resolution (higher Q_{ADC} and smaller DC gain) leads to smaller DLDO bandwidth, and in some cases, DLDO loop may not even respond to small changes in the encryption current as ADC output doesn't change unless change in V_{OUT} is more than 1 ADC bin. For very poor ADC resolution, feedback loop is always non-responsive with direct path through power-stage with a R-C low pass filtering determining the output voltage. For these cases, I_{IN} is low-pass filtered version of I_{ENC} with high frequency signature attenuation (no signal distortion that is attributed to DLDO feedback loop). An interesting trend is observed when sampling frequency (F_s) of the feedback loop is varied. For very low F_s, the DLDO loop responds very slowly, with R-C filter dominating the immediate response (therefore only attenuation is observed with small or no signal distortion) leading to higher SNR compared to nominal case. However, as F_s is increased, the DLDO feedback loop with higher bandwidth starts responding adding quantization losses and signal distortion. For very high F_s, the DLDO feedback loop can respond very fast and very accurately and therefore increasing the SNR in I_{IN}. Compensator PID gains have negligible impact on SNR. Fig. 7.12 shows that even with varying gains, the response of DLDO during the targeted round of the encryption is similar therefore producing same SNR results. Very similar trends are observed for CPA MTD.

7.4 Experimental Setup and SCA Methodology

Fig. 7.13(a) & (b) show 1mm$\times$2mm testchip [67] fabricated in 130nm CMOS consisting of digital LDO with proposed SNI and R-VREF circuits, AES and SIMON cores and key design details [143]. Fig. 7.13(c) shows the measurement framework. The nominal operating conditions for encryption cores in standalone mode (without DLDO) are $\sim$ 62MHz @0.84V. When ADCM is enabled, these cores can run at $\sim$ 80MHz at 0.84V. Test-board fabricated to measure the side channel activity is shown in Fig. 7.14(a). Power signa-

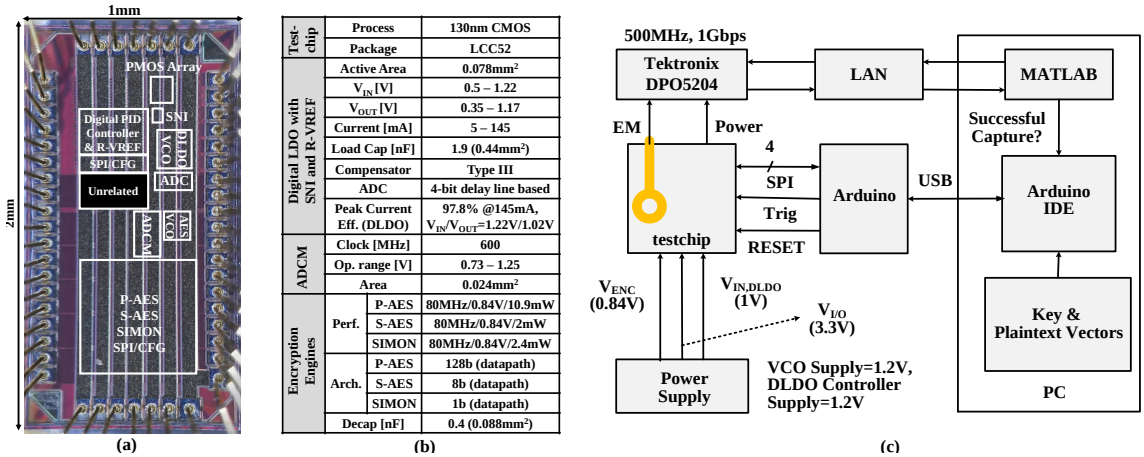


Figure 7.13: (a) Die photo, (b) details of the testchip and (c) measurement setup.

tures are captured at both $V_{IN,DLDO}$ and V_{ENC} across a 1Ω resistor while EM emanations are acquired with EMC probe (Beehive EMC probe 100A, loop diameter: 0.4", 3dB bandwidth: 1GHz) [98] near V_{ENC} and $V_{IN,DLDO}$ [Fig. 7.14(b)]. The external trigger used to start encryption is also used to trigger Tektronix DPO5204 oscilloscope (2GHz bandwidth, 10Gbps max sampling freq.) at 1Gbps sampling rate and 500MHz bandwidth.

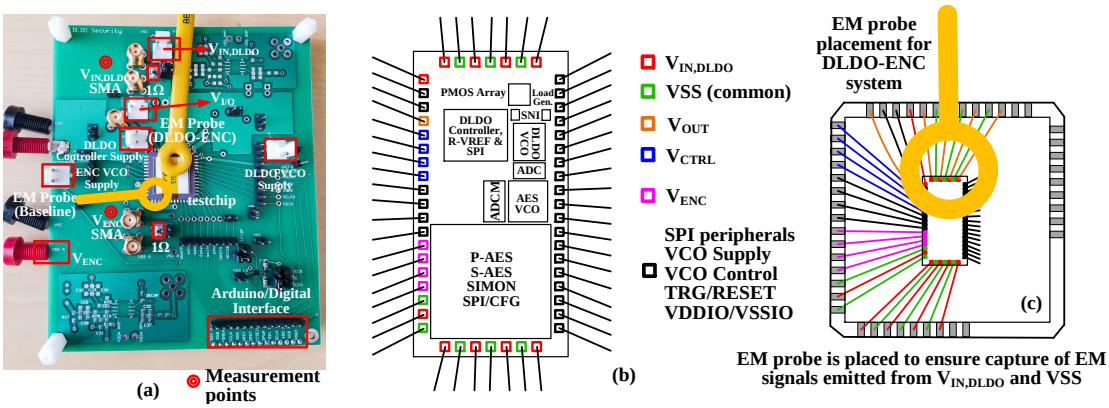


Figure 7.14: (a) Test-board manufactured to measure side channel activity, (b) pinout specifications for the testchip showing the power, ground pins critical for EM signature acquisition with respect to probe placement and signal isolation.

7.4.1 Measurement Scenarios

Baseline

Encryption cores are powered from external supply (0.84V) and run at fixed clock freq. ($\sim$ 62MHz). Both DLDO and ADCM are turned off. Power/EM signatures are measured at V_{ENC}.

DLDO-ENC System

Encryption cores are powered from the output of digital LDO at a fixed supply (0.84V) and fixed clock ($\sim$ 62MHz). ADCM is turned off. Power/EM signatures are captured at $V_{IN,DLDO}$.

DLDO-ENC System with SNI & R-VREF (DLDO-ENC-SR System)

Both SNI & R-VREF are enabled for DLDO-ENC system. Signatures are captured at $V_{IN,DLDO}$. Intermediate design points with only SNI (DLDO-ENC-S) and only R-VREF (DLDO-ENC-R) are also analyzed.

SNI when enabled creates voltage noise ranging from 0.75V to 0.98V with several large spikes [Fig. 7.15(a)]. However, average voltage noise added over AES clock period is small and therefore, ADCM generates only slightly lower (vs nominal) freq. levels ranging from 64MHz to 79MHz with mean freq. of 72.5MHz. Similarly, with R-VREF turned on, the voltage varies from 0.79V to 0.88V (90mV total) and corresponding clock varies from 66MHz to 86MHz (mean freq. of 79.1MHz) [Fig. 7.15(b)]. Fig. 7.16 shows the load transient response for the nominal DLDO for a 40mA load step (5mA to 45mA in 100ps). For the selected PID gains [22/32, 24/32, 9/32], the measured response is slightly underdamped.

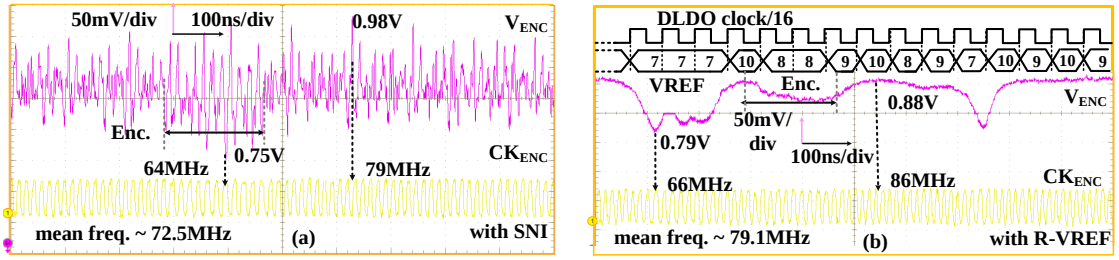


Figure 7.15: Measured circuit operation for (a) SNI and (b) R-VREF with respect to supply voltage (V_{ENC}) and clock (CK_{ENC}) inputs to encryption cores. SNI is enabled with highest possible width for pulse out and R-VREF is run at DIV16 of DLDO clock.

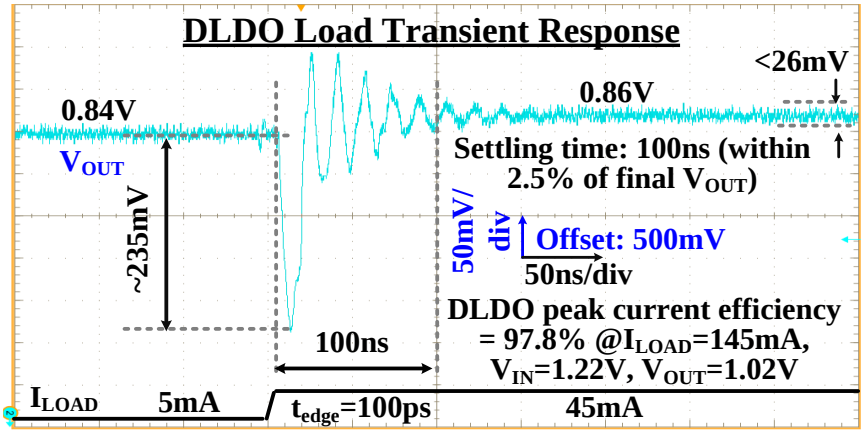


Figure 7.16: Measured load transient response for the nominal DLDO with ΔI_L=40mA/100ps @V_{IN}=1.0V, V_{OUT}=0.84V.

7.4.2 SCA Methodology

Two tests are employed to quantify the effectiveness of proposed countermeasures- 1) TVLA and 2) CPA (CEMA). Both of these tests have been presented in Chapter 3 but are briefly described below:

TVLA

TVLA is a standard statisitcal hpyothesis testing methodology to validate SCA resistance offered by a countermeasure [76]. In our experiments, with TVLA, a t-statistic based on Weltch's t-test is computed in both time and freq. domain using 100000 measurements. A t-statistc of more than $\pm$4.5 indicates leakage with 99.9999% confidence. Compared to our prior work in [100], only 1st order TVLA is used.

CPA & CEMA

As described in Chapter 3.2.2, both correlation power analysis (CPA) and correlation EM analysis (CEMA) is performed on the measured power and EM signatures. Upto 10 million measurements are collected to evaluate the success of the proposed countermeasures. Both CPA/CEMA are also analyzed in frequency domain as well.

7.4.3 Postprocessing of Measured Traces

Fig. 7.17 shows the postprocessing methods used to filter and align the measured signatures. TVLA and CPA tests are subsequently carried out on the filtered and aligned signatures in both time and freq. domains. Fig. 7.18(a) shows the captured signatures for P-AES

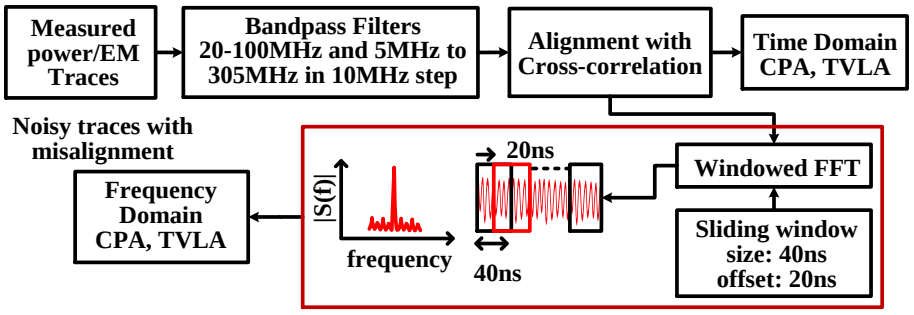


Figure 7.17: Postprocessing including filtering and alignment of captured signatures and SCA analysis in time and frequency domains.

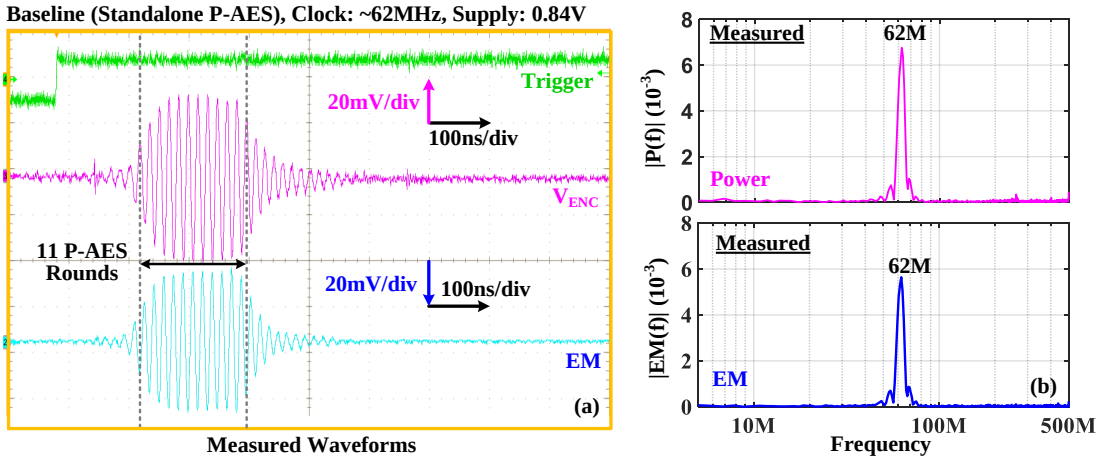


Figure 7.18: Baseline (standalone P-AES) system: (a) measured waveforms captured at/near V_{ENC} and (b) their spectral characteristics. Both DLDO and ADCM circuits are turned off.

at V_{ENC}, all 11-rounds of operation are clearly observed. A spectral peak is observed at the clock freq. (62MHz) in the FFT of these signatures [Fig. 7.18(b)]. Other spectral peaks are considerably smaller. Power/EM signatures have similar spectral content (strength, frequencies). Fig. 7.19(a) shows the measured signatures for DLDO-ENC and DLDO-ENC-SR systems. For DLDO-ENC system, the measured power/EM signatures show clear peaks but significant signal distortion/attenuation is observed, also demonstrated by the spectrum [Fig. 7.20(a)]. For DLDO-ENC-SR system, the peaks are no longer observable in power signature which is flattened [Fig. 7.19(b)]. EM signature shows slightly better charac-

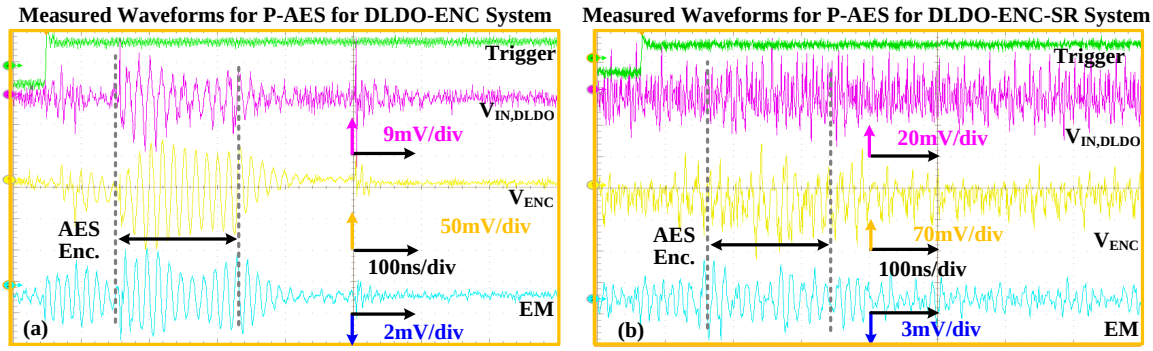


Figure 7.19: Measured power/EM signatures for P-AES for (a) DLDO-ENC and (b) DLDO-ENC-SR systems.

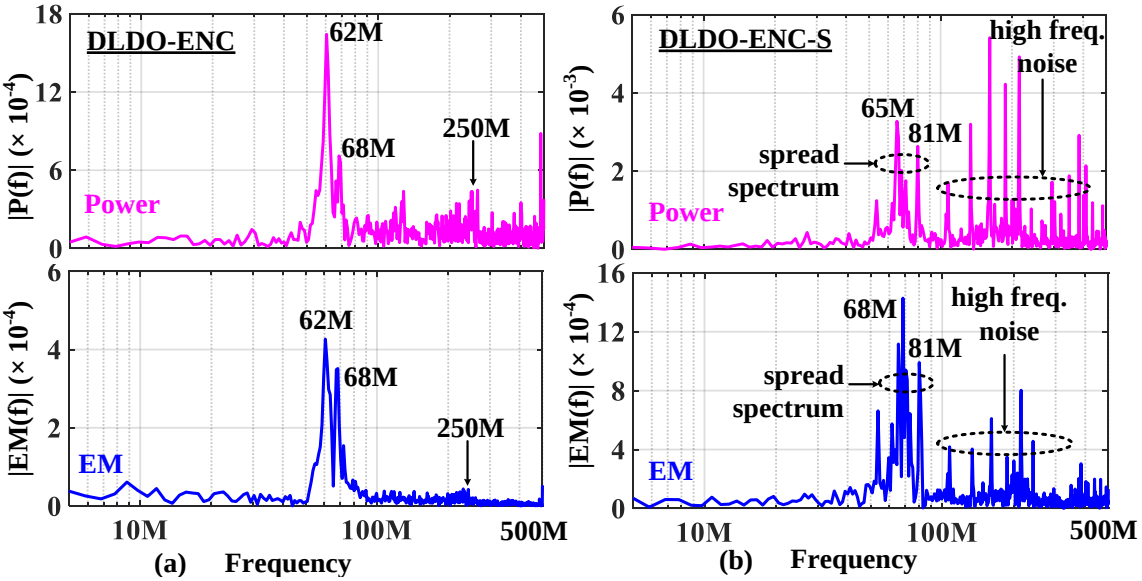


Figure 7.20: Spectral characteristics of measured signatures for P-AES for (a) DLDO-ENC and (b) DLDO-ENC-S systems.

teristics with observable peaks during the encryption (attributed to EM emanations from on-chip power grid as well as the ground node of the chip), however, its strength is much weaker than power signature. Spectra of these signatures show freq. spreading for both SNI and R-VREF [Fig. 7.20(b) & 7.21(a)]. SNI adds several peaks in high freq. bands commensurate to DLDO clock freq. while R-VREF causes freq. spreading near encryption clock freq. (F_{ENC}), therefore, suppressing signals in both low and high freq. regions leading to reduction in SNR when both are enabled [Fig. 7.21(b)].

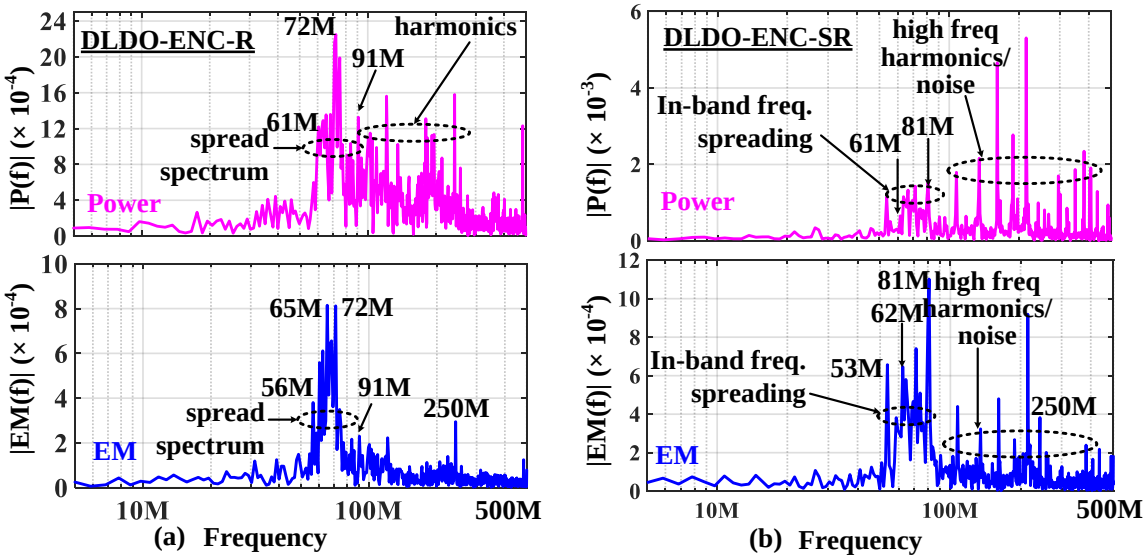


Figure 7.21: Spectral characteristics of measured power/EM signatures for P-AES for DLDO-ENC with (a) R-VREF enabled and (b) with both SNI & R-VREF enabled.

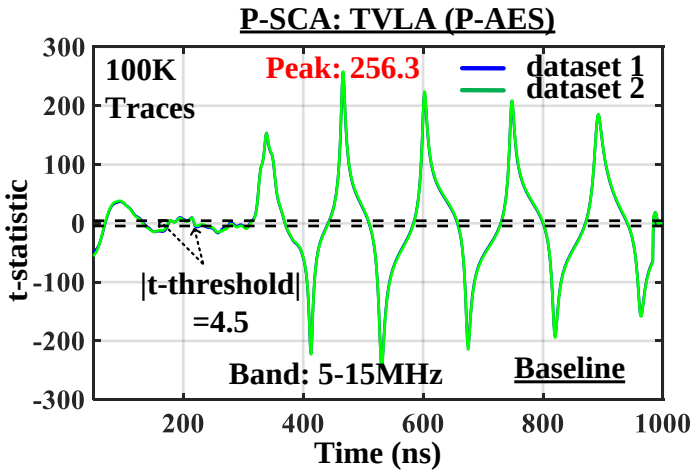


Figure 7.22: TVLA analysis for P-AES for baseline (standalone) system.

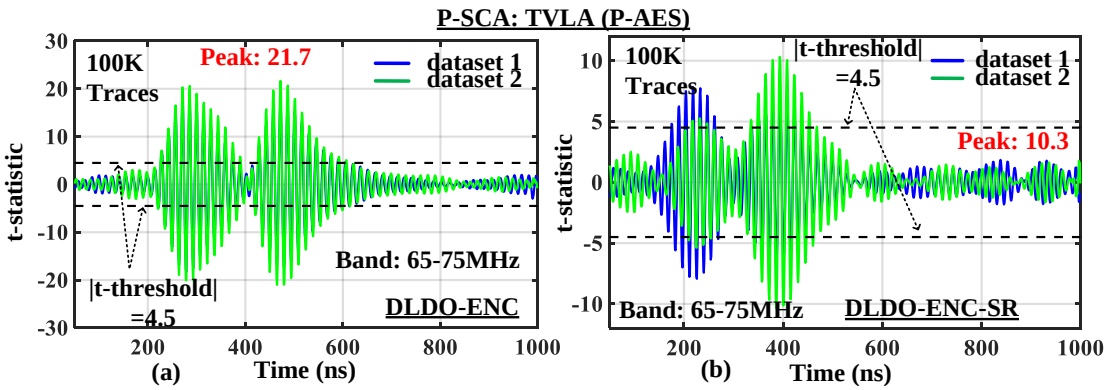


Figure 7.23: TVLA analysis for P-AES for (a) DLDO-ENC and (b) DLDO-ENC-SR systems.

7.5 Measured SCA Results: Power and EM SCA

7.5.1 Power Side Channel Analysis (P-SCA) on P-AES

TVLA Analysis

For TVLA analysis, the worst case TVLA peak across time and freq. *[max(|t-statistic(time)|, |t-statistic(freq)|)* is considered for comparison.

Baseline System

T-statistic for the baseline system at $V_{IN,DLDO}$ node plotted against time in Fig. 7.22 shows high levels of leakage for unprotected P-AES system (peak of 256.3) in 5MHz-15MHz band. Freq. domain TVLA shows slightly higher TVLA peak (258) [Table 7.3]. High levels of leakage are also observed across all filter bands with higher leakages observed at low freq. bands indicating low freq. components tend to carry more information than high freq. components [Fig. 7.24].

DLDO-ENC System

For the DLDO-ENC system, TVLA analysis performed at $V_{IN,DLDO}$ shows that t-statistic in time domain is significantly reduced [Fig. 7.23(a)] to 21.7. Leakage reduces in most of the filter bands but most of the reduction occurs at low freq. bands [Fig. 7.24]. Reduction in

TVLA peak can be attributed to inherent freq. dependent transformations induced by the DLDO in the encryption currents. Also as highlighted in Fig. 7.19(a), signal distortions due to close loop operation of the DLDO help in reducing the information leakage. Since the bandwidth and phase margin of the DLDO is dependent on PID gains, changing these gains modulates the TVLA leakage [Table 7.3]. For larger PID gains, the feedback path through the controller plays a big role as it responds to transient load currents and controller losses due to sampling freq., ADC and power-stage quantization affect the TVLA leakage. In contrast, DLDO with smaller bandwidth cannot respond to high freq. signatures making the direct leakage path from V_{OUT} to $V_{IN,DLDO}$ through power-stage prominent. Note that we saw no/negligible impact of PID gains on SNR or CPA MTD from simulations. The reason behind contrasting results between simulations and measurements is difference in SCA metric. Unlike SNR/CPA, TVLA measures the SCA leakages during intermediate rounds of computations (round 3-7 for P-AES). In Fig. 7.12 we saw that I_{IN} during intermediate rounds of P-AES are modified through DLDO when we vary PID gains while last round has negligible/no changes.

DLDO-ENC-SR System

For the DLDO-ENC-SR system, the TVLA leakage in time domain further reduces to 10.3 (leakage in freq. domain=9.95) indicating a total reduction of 25.1$\times$ [Fig. 7.23(b)]. Leakage in most of the filter bands reduces below the threshold of 4.5 [Fig. 7.24].

Table 7.3 illustrates the impact of SNI & R-VREF circuits separately and explores impact of different settings (pulse width for SNI and LFSR clock freq. for R-VREF). For SNI, reduced TVLA leakages are observed when SNI pulse width is increased. Similarly, for R-VREF, an intermediate clock freq. for LFSR relative to encryption clock freq. as well as DLDO bandwidth is ideal to achieve good randomization of the supply voltage and clock freq. Table 7.3 shows that DIV16 setting for the LFSR clock has smaller TVLA leakage than DIV64 setting.

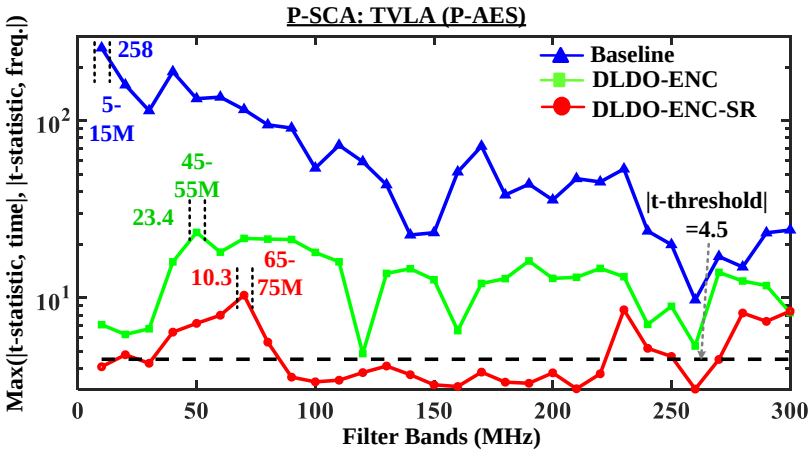


Figure 7.24: TVLA peak vs filter bands show reduced leakage across all bands for DLDO-ENC system which further reduces for DLDO-ENC-SR system.

Table 7.3: Comparison of different configurations with respect to TVLA leakage.

Circuit Technique		Configurations	TVLA Leakage		Max TVLA
			Time	Freq.	
Baseline P-AES		-	256.3	258	258
DLDO-ENC for P-AES	PID Controller	22/32, 24/32, 9/32*	21.7	23.4	23.4
		10/32, 7/32, 2/32	25.2	24.3	25.2
		0, 1/32, 0	31.7	32.9	32.9
	LFSR clock for R-VREF	DIV16*	9.9	13.1	13.1
		DIV64	17	17.4	17.4
	Pulse width for SNI	$T_{clock}/9$	14	15.3	15.3
		$2T_{clock}/9$	13.7	11.7	13.7
		$3T_{clock}/9$*	11.9	11.4	11.9

*configuration selected in this work for SCA analysis unless stated specifically

CPA Analysis

Baseline System

Fig. 7.25(a) & (b) show time/freq. domain CPA for byte 9 of the key (highest leaking byte) for baseline P-AES system with 10K traces. Correct subkey is revealed in both time/freq. domains. Peak correlation plotted against # of measurements for freq. domain CPA in Fig. 7.26(a) shows an MTD of only 400 measurements. MTD for time domain CPA is 800 measurements. Since freq. domain CPA always provides better results, the subsequent sections will only focus on freq. domain CPA with time domain results summarized later

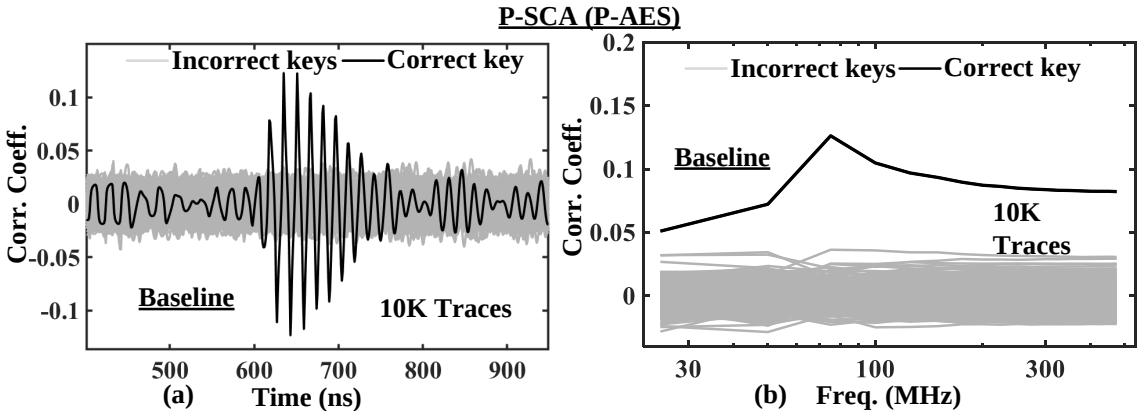


Figure 7.25: CPA attack results for P-AES for Byte 9 for baseline system in (a) time domain, (b) freq. domain with 10K traces.

in this chapter. CR for byte 9 is plotted against filter bands in Fig. 7.29 for 5 million measurements. It shows that correct subkey can be recovered from all filter bands indicating information leakage across the entire frequency spectrum. SR plotted in Fig. 7.28(c) shows that 80% of all subkeys can be recovered with only 1900 measurements.

Effect of Power Gate and Decoupling Capacitance

When P-AES is powered externally through V_{OUT} (DLDO, R-VREF, SNI are off) to emulate a design with an on power gate (test-control switch) with 1.9nF decoupling capacitor on the ungated input rail and 0.4nF on the virtual rail [Fig. 7.27(a)], the MTD increases to only 2200 from 400 for byte 9. Similarly, MTD for 80% SR for CPA and CEMA increases to 4800 from 1900 for P-AES [Fig. 7.27(b)]. Therefore, when on-chip decoupling capacitor is increased from 0.4nF to 1.9nF+0.4nF (2.3nF total), the total decoupling capacitor along with test-control switch with its finite resistance acts as a low pass filter. Some of the high frequency components are filtered out but since most of the leakage is concentrated in low freq. region, overall SCA leakage characteristics do not change significantly.

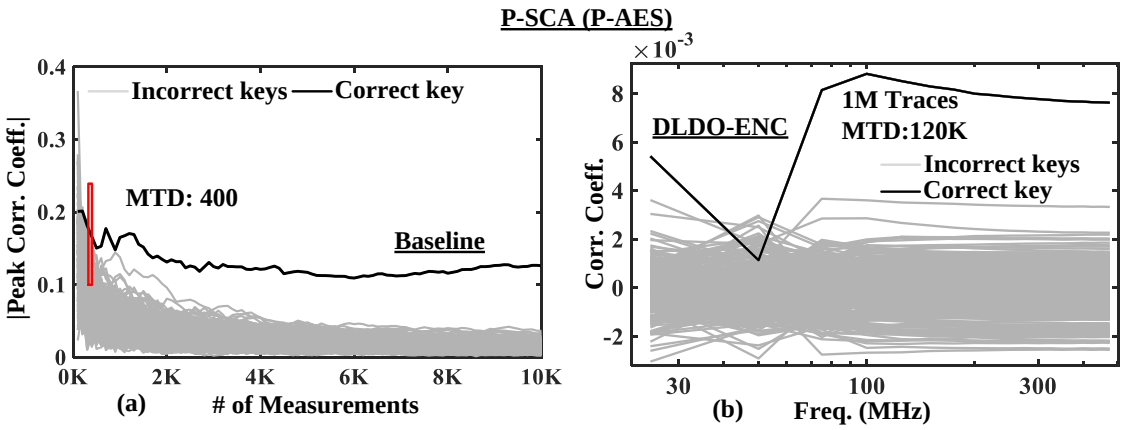
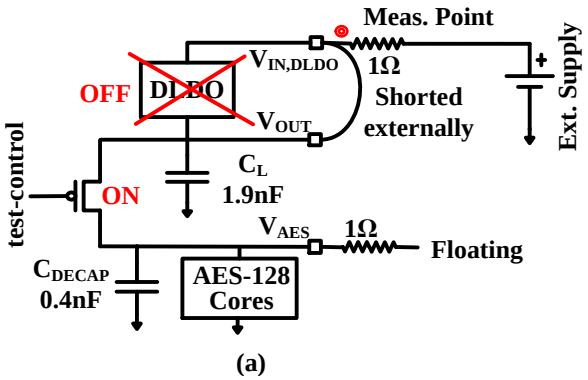


Figure 7.26: Freq. domain CPA attack results for Byte 9 for P-AES for (a) baseline system with MTD of 400 traces in (MTD=800 in time domain) and (b) correlation vs freq. for DLDO-ENC system.



Total On-Chip Decoupling Capacitor	MTD for 80% SR	
	P-AES	S-AES
0.4nF	1900	3300
2.3nF	4800	5500

(b)

Figure 7.27: Effect of test-control power gate and on-chip decoupling capacitance on CPA/CEMA results (a) measurement configuration and (b) MTD for 80% SR for the baseline P-AES shows small impact of on-chip decap (0.4nF vs 2.3nF).

DLDO-ENC System

CPA performed for DLDO-ENC system shows that byte 9 can be recovered with 120K measurements (an increase of 300× with respect to baseline) []Fig. 7.26(b)]. Like baseline system, CR plot in Fig. 7.29 shows that most of the filter bands can be used to reveal the correct subkey. Fig. 7.28(b) shows that MTD for 80% SR is 320K (increased by 168× with respect to baseline).

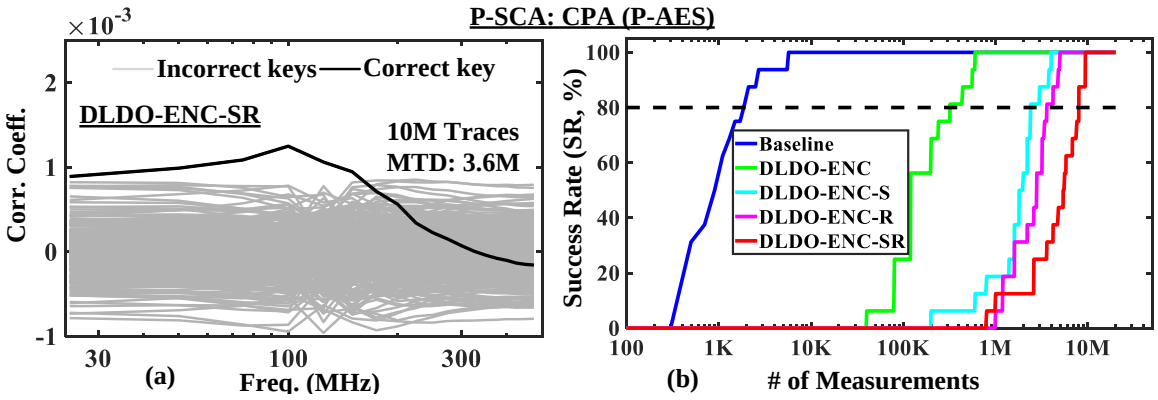


Figure 7.28: Freq. domain CPA attack results for P-AES for Byte 9 for (a) DLDO-ENC-SR system and (b) SR vs # of measurements.

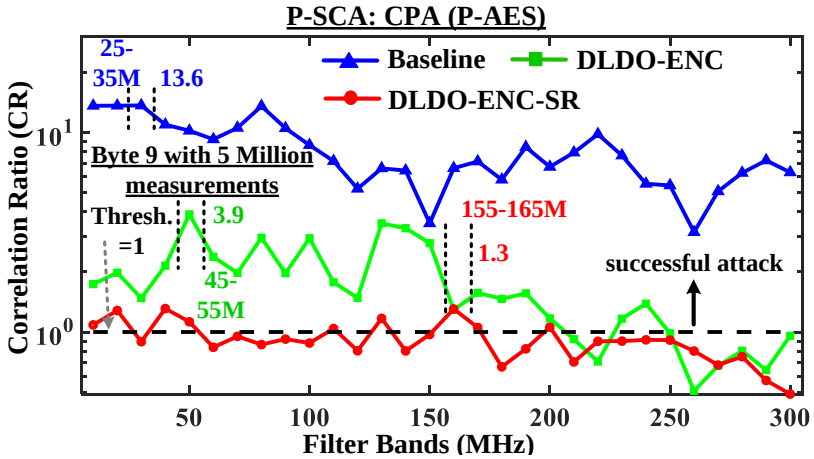


Figure 7.29: CR plotted against filter band shows large leakage in all bands for baseline system which reduces for DLDO-ENC and DLDO-ENC-SR systems.

DLDO-ENC-SR System

For the DLDO-ENC-SR system, byte 9 can still be revealed, however, the number of measurements required increase to 3.6 millions (9000× with respect to baseline) [Fig. 7.28(a)]. MTD for 80% SR increases to 8 million (4210× over baseline) [Fig. 7.28(b)].

With only SNI or only R-VREF enabled for DLDO-ENC system, CPA MTD for 80% SR is 2.4 millions or 3.6 millions respectively [Fig. 7.28(b)]. SNI adds significant high freq. noise (determined by F_{DLDO} and its transient response) while signal scrambling near F_{ENC} is small as average noise added during each encryption clock cycle doesn't cause critical path delay deviate too much from its nominal value. However, with R-VREF since

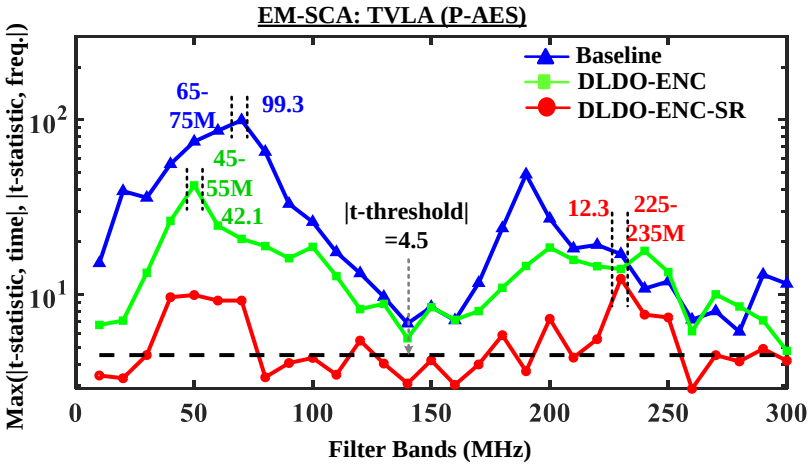


Figure 7.30: TVLA leakage vs filter bands for EM-SCA shows reduced leakage for DLDO-ENC-SR system, however, leakage is higher than P-SCA.

supply voltage is modulated at lower speed (250MHz/16 $\approx$ 16MHZ), ADCM generates F_{ENC} with larger variations. SNI & R-VREF together help in suppressing leakage across entire freq. spectrum [Fig. 7.29]. Additionally, even though TVLA analysis shows SNI is more effective vs R-VREF [Table 7.3], CPA analysis shows opposite trends [Table 7.5].

7.5.2 EM Side Channel Analysis (EM-SCA) for P-AES

EM emissions from digital gates, on-chip wires, PDN and decoupling capacitances have been demonstrated to be dependent on intermediate variables [5] and in certain cases carry more information than power side channel, especially in the presence of countermeasures [100]. Since our proposed circuits randomize the power consumption of the AES core by modulating both supply and clock inputs, the EM emanations should also be randomized leading the reduction in information leakage. This section analyzes and quantifies reduction in EM side channel leakage with the proposed circuit techniques.

TVLA Analysis

Fig. 7.30 plots t-statistic across filter bands for all systems. The baseline system has large leakage with peak=99.3 which reduces to 42.1 for DLDO-ENC system. With respect to P-SCA, EM-SCA has smaller leakage for baseline (258 vs 99.3) but much higher leakage for

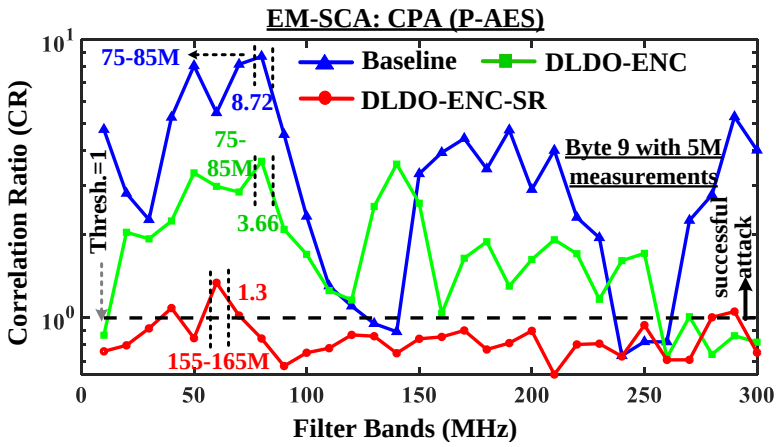


Figure 7.31: CR plotted against filter bands for EM-SCA shows similar peak value as P-SCA for DLDO-ENC-SR system however the highest leaking bands are different.

DLDO-ENC (23.4 vs 42.1) system. For the DLDO-ENC-SR system, the TVLA leakage further reduces to 12.3 indicating a total reduction of 8.2×. Compared to P-SCA which only captures side channel leakage through current measured at $V_{IN,DLDO}$, localized EM-SCA (near $V_{IN,DLDO}$) also captures side channel leakage from VSS pins, local PDN (output of the DLDO) and therefore has significantly higher TVLA peak for the DLDO-ENC system. Both SNI and R-VREF randomize supply and clock therefore randomizing the current drawn from encryption core via V_{ENC} which is subsequently discharged to VSS. Therefore, for the DLDO-ENC-SR system, EM-SCA has comparable peak as P-SCA (12.1 vs 10.3).

CEMA Analysis

Key recovery attacks with respect to CEMA show that both baseline and DLDO-ENC systems leak across most of the filter bands [Fig. 7.31]. The leakage for the DLDO-ENC-SR is constrained to only few bands demonstrating similar characteristics as CPA. However, SR plot in Fig. 7.32 shows that it's harder to reveal subkeys for the baseline but easier for the DLDO-ENC-SR system (MTD for 80% SR = 7.2 millions, an increase of only 136× with respect to baseline for CEMA, much smaller than 4210× observed with respect to CPA). Both SNI & R-VREF show similar individual trends as observed for CPA with R-VREF slightly more effective vs SNI.

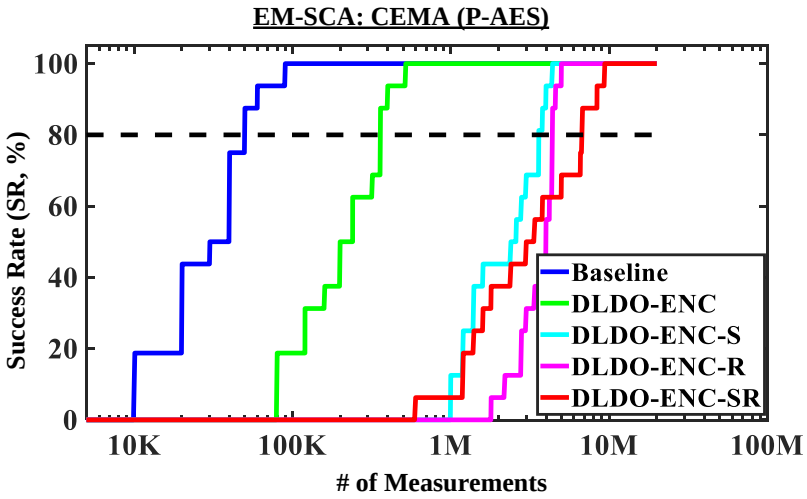


Figure 7.32: SR plotted against # of measurements shows subkeys are easier to recover with respect to CEMA than CPA for DLDO-ENC-SR system. However, it still takes 7.2M measurements to reveal 80% of the subkeys.

7.5.3 Role of Limit Cycle Oscillations (LCO)

Digital LDOs suffer from steady-state limit cycle oscillations (LCO), especially at light load conditions due to inherent quantization errors of the loop components (ADC and DAC). Under certain operating conditions (input supply, load current and PID gains), the DLDO can go into LCO even at slightly higher currents. We reduced the base current at the output (through load generators) to 5mA to force the DLDO into LCO at different output voltages (0.79V, 0.85V, 0.88V), With LCO, the output starts oscillating at a cer-

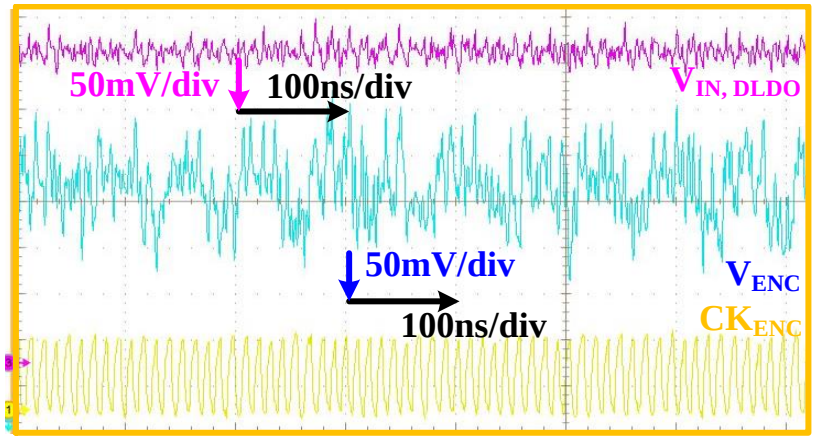


Figure 7.33: Measured power waveforms at V_{ENC}, $V_{IN,DLDO}$ and encryption clock under LCO at V_{ENC}=0.88V at a base current of 5mA. ADCM is on.

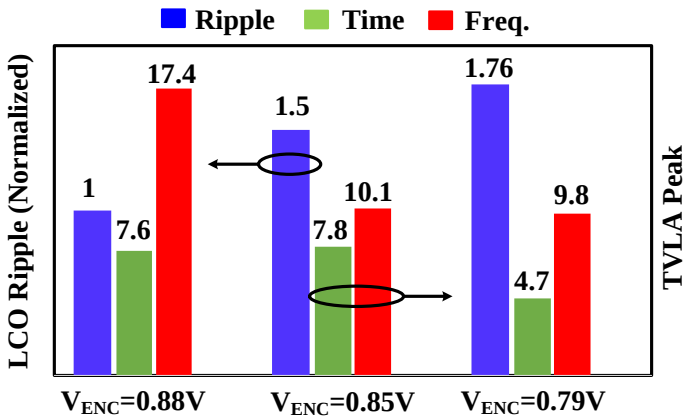


Figure 7.34: Effect of LCO on TVLA leakage time time/freq. domains at light load current ($I_{base} \sim 5mA$) and different V_{ENC} settings.

tain frequency depending on the LCO mode. With ADCM turned on, both V_{ENC}/F_{ENC} are modulated [Fig. 7.33]. Large ripple is added at the output and the pattern of the oscillations depend on the LCO mode which in turn depends on the operating conditions. Fig. 7.34 shows the reduction in TVLA peak that can be obtained with LCO with higher ripple leading to smaller TVLA leakage. With ADCM, even with very high LCO ripple, the impact on performance is small (66MHz nominal vs 65.2MHz with LCO for V_{ENC}=0.79V, 1.2% degradation) since the mean voltage remains close to nominal voltage. CPA (CEMA) analysis shows MTD for 80% SR of 3.2 (8) millions in freq. domain for V_{ENC}=0.79V. In summary, LCO shows better (similar) improvement compared to SNI & R-VREF for TVLA (CPA) but provides much higher resistance for CEMA due to DLDO dominating the EM emission because of higher ripple.

Table 7.4: TVLA leakage analysis under power injection attacks at $V_{IN,DLDO}$ and V_{CTRL}.

Time/ Freq.	TVLA Leakage under Power Injection Attack (PIA) with Reduced Voltage at DLDO Input ($V_{IN,DLDO}$) and Controller Supply (V_{CTRL})					
	Power Analysis			EM Analysis		
	w/o PIA	Under PIA		w/o PIA	Under PIA	
		$V_{IN,DLDO}$- 80mV	V_{CTRL}- 100mV		$V_{IN,DLDO}$- 80mV	V_{CTRL}- 100mV
Time	10.35	9.9	5.5	9.7	23.6	6.2
Freq.	9.95	10.9	5.8	12.3	20.9	7.7

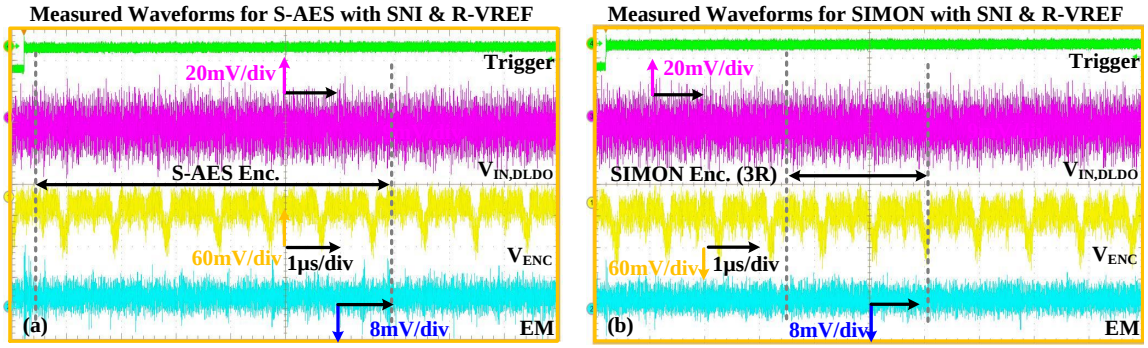


Figure 7.35: Measured power/EM signatures for DLDO-ENC-SR system for (a) S-AES and (b) SIMON encryption cores. For SIMON core, only initial 3 rounds (3R) of encryption are shown.

7.5.4 Power Injection Attack (PIA)

A power injection attack (PIA) with a voltage glitch [141] is performed at V_{CTRL} (control supply that powers the DLDO loop, R-VREF, SNI, and LFSRs), and $V_{IN,DLDO}$. The PIA at V_{CTRL} introduced instability/noise at V_{ENC} forcing random clock-skipping from ADCM, which de-synchronizes power/EM signatures [with 100mV glitch TVLA reduced to 5.8 (power) and 7.7 (EM)] but degrades encryption throughput [Table 7.4]. A PIA on $V_{IN,DLDO}$ can cause all power PMOSs to be always ON, rendering DLDO and R-VREF in-effective, but SNI remains effective; MTD for 80% SR of 8.4M (power) and 6.0M (EM) are observed for an 80mV glitch [Table 7.4]. The security of DLDO-ENC can be further improved by using a TRNG to reduce predictability/repeatability of LFSR and adding input sensing circuits at $V_{IN,DLDO}$ and V_{CTRL} to inhibit a PIA [141].

7.5.5 Power and EM SCA on S-AES and SIMON

To understand the effectiveness of proposed circuit techniques across algorithms and datapath architectures, SCA is performed on both S-AES and SIMON. Fig. 7.35(a) & (b) show the measured power/EM signatures for S-AES and SIMON engines respectively for DLDO-ENC-SR system. Only CPA and CEMA experiments are carried out for S-AES and SIMON. Also for SIMON, only baseline and DLDO-ENC-SR systems are analyzed.

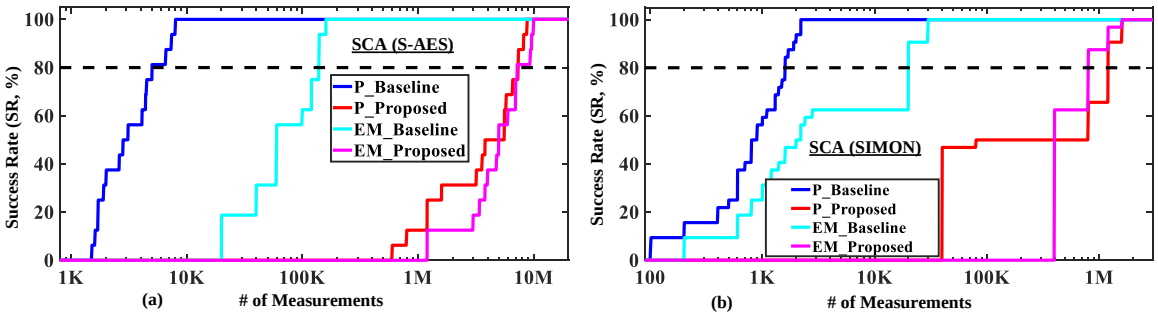


Figure 7.36: SR plotted against # of measurements for baseline and proposed systems with respect to power (P) and EM SCA for (a) S-AES (b) SIMON cores.

Table 7.5: Summary of CPA/CEMA attacks for AES cores for different systems with respect to MTD for 80% SR.

AES core	System (S=SNI, R=R-VREF)	CPA		CEMA	
		Time	Freq.	Time	Freq.
P-AES	Baseline	3100	1900	80K	50K
	DLDO-ENC	0.68M	0.32M	0.84M	0.36M
	DLDO-ENC-S	4.2M	2.4M	>5M* (7)	3.6M
	DLDO-ENC-R	>5M* (7)	3.6M	>5M* (4)	4.4M
	DLDO-ENC-SR	>10M* (7)	8M	>10M* (11)	6.8M
S-AES	Baseline	5000	3300	>200K* (7)	140K
	DLDO-ENC	1M* (6)	0.96M	>1M* (2)	0.88M
	DLDO-ENC-S	>5M* (11)	3.6M	>5M* (7)	3M
	DLDO-ENC-R	>5M* (2)	4M	>5M* (1)	3.8M
	DLDO-ENC-SR	>10M* (9)	7.4M	>10M* (4)	7.2M

*** 80% of the subkeys could not be revealed with given number of measurements. # of subkeys that could be revealed are given in the bracket.**

SCA on S-AES

For P-SCA, MTD for 80% SR for the baseline system is 3300 which increases to 0.96 millions for DLDO-ENC (291×) and 7.4 millions for DLDO-ENC-SR (2242×) systems [Fig. 7.36(a)] [Table 7.5]. For EM-SCA, MTD for 80% SR for the baseline system is 140000 which increases to 0.88 millions for DLDO-ENC (an increase of only 6.3× over baseline) and 7.2 millions for DLDO-ENC-SR (an increase of only 51.4× over baseline) systems [Fig. 7.36(a)].

Table 7.6: Summary of improvement in SCA resistance (with respect to MTD for 80% SR) for AES & SIMON with the proposed countermeasure.

Encryption Core		P-AES		S-AES		SIMON	
System		Base-line	Pro-posed	Base-line	Pro-posed	Base-line	Pro-posed
CPA	Time	3100	>10M	5000	>10M	8200	5.2M
	Freq.	1900	8M	3300	7.4M	1600	1.2M
CEMA	Time	80K	>10M	>200K	>10M	>200K	2.8M
	Freq.	50K	6.8M	140K	7.2M	20K	0.8M

SCA on SIMON

For P-SCA, MTD for 80% SR for the baseline system is 1600 which increases to 1.2 millions for DLDO-ENC-SR (750×) system [Table 7.6] [Fig. 7.36(b)]. For EM-SCA, MTD for 80% SR for the baseline system is 20000 which increases to 0.8 millions for DLDO-ENC-SR (an increase of only 40× over baseline) system.

Discussion on SCA Improvement for Different Encryption Cores

Table 7.6 summarizes the CPA/CEMA analysis results with respect to SR for baseline and proposed countermeasure for P-AES, S-AES and SIMON cores in time and freq. domain. For cases where 80% subkeys could not be recovered, number of subkeys recovered with given number of measurements are presented (out of 16 for P-AES and S-AES, out of 32 for SIMON). When we compare the two AES cores, MTD for 80% SR for both AES cores shows similar trends for either baseline (3300 for S-AES vs 1900 for P-AES) or DLDO-ENC-SR (7.4 millions for S-AES vs 8 millions for P-AES) systems with respect to CPA. Intermediate systems as well as CEMA analysis show more or less similar trends. When we analyze the leakage behavior for SIMON vs AES cores, we see very different results for DLDO-ENC-SR system. Only 1.2 million measurements are required for revealing 80% subkeys for SIMON vs 8 million measurements required for P-AES with respect to CPA (similar trends for CEMA). This difference in side channel leakage characteristics can be attributed to two different factors- 1) hardware architecture and 2) choice of leakage

models. Both AES cores are implemented in such a way that for each subkey, leakage is generated only when that subkey is used in the datapath in "a single cycle". For SIMON, due to use of shift registers [Fig. 3.4], the computed sensitive bit is shifted through each flip-flop in the shift-register generating leakage in 64 clock cycles increasing probability of successful attack. Another reason for reduced impact of proposed countermeasure for SIMON is the choice of leakage model. For SIMON, 1-bit models are chosen compared to 8-bit models for AES cores. 1-bit power models have been shown to be more effective in certain cases [144].

7.5.6 Overhead Analysis for the Proposed Countermeasure

For overhead analysis, only P-AES core has been considered. Design overheads are discussed as follows:

Area Overheads

The total silicon area for P-AES is 0.275 mm^2. The proposed countermeasure consumes 0.101 mm^2 including DLDO, SNI, R-VREF and ADCM circuits (total 36.9% of P-AES area). For DLDO, the area for power-stage, ADC, and controller are included.

Performance Overheads

DLDO-ENC system is designed to run at the same freq. as the baseline system indicating no performance loss. For DLDO-ENC-SR system, R-VREF scheme is designed such that an average system throughput (same as baseline system) is maintained over long period of time therefore resulting in very small performance loss (1.1%). SNI incurs an additional 9.3% and therefore total performance loss is only 10.4%.

Table 7.7: Comparison with prior works on circuit based SCA countermeasures.

Metric		This Work	JSSC'18 [128]	JSSC'19 [100]	VLSI'15 [29]	ISSCC'09 [21]	ISSCC'18 [141]	ISSCC'11 [27]
Countermeasure Technique		On-chip Digital Low Dropout Regulator with SNI & R-VREF	Integrated Buck Regulator	Random Fast Voltage Dithering	Charge Recovery Logic	Switch Capacitor Current Equalizer	Buck Regulator	Duplicated Complement -ed Logic
Technology		130nm	130nm	130nm	65nm	130nm	55nm	130nm
AES power[a]		10.9mW @ 80MHz, 0.84V	10.5mW @40MHz	13.1mW @49.7MHz	138mW @1.32GHz	33mW @100MHz	No AES/other Encrypt-ion Engine present	- @50MHz
Design Overheads[a]	Area	36.9%b	1%c	6.6%c	25%	33%		104%
	Power	32%b	5%c	3.5%c	30%	20%		-
	Perf.	10.4%	3.33%	17.4%	0%	50%		0%
# of Measurements		10M	500K	1M	1M	10M	N/A[e] (No SCA)	1M
SCA Analysis[d]	Time/Freq. Domain	Time, Freq.	Time, Freq.	Time, Freq.	Time	Time		Time
	MTD for 80% SR	6.8M (3579×)[f]	>500K (100×)[g]	>500K (692×)[g]	940K (251×)[h]	>10M (2500×)[i]		800K
	Attack Mode	Power, EM	Power, EM	Power, EM	Power	Power		Power, EM

[a]With respect to parallel AES (P-AES). [b]Includes DLDO regulator area/power. [c]Doesn't include regulator area/power.
[d]For P-AES. [e]Relative correlation based analysis. [f]Minimum of CPA MTD and CEMA MTD.
[g]SCA performed for only 1 byte. [h]MTD to disclose all bytes. [i]None of the bytes could be disclosed.

Power Overheads

Measured power consumption for baseline P-AES is 10.9mW at 80MHz, 0.84V. For DLDO-ENC-SR system, assuming total load current of $\sim$ 40mA, DLDO provides 68% power-efficiency when SNI and R-VREF circuits are enabled with ADCM indicating a power loss of 32%.

Comparison with Prior Works

Comparison with prior work is presented in Table 7.7 with focus on circuit/logic-level countermeasures, similar in nature to this work. For comparison, minimum MTD for 80% SR across CPA/CEMA is used assuming an adversary can perform both CPA/CEMA. The proposed countermeasure achieve 3579×, 2182× and 500× increase in MTD for 80% SR across CPA & CEMA for P-AES, S-AES and SIMON cores respectively. Unlike the prior work in [128][141], the proposed countermeasure doesn't require any large passives and unlike [100], it can randomize signatures even during the same encryption achieving greater SCA resistance. The proposed countermeasure can also be integrated with other hiding [29][27] and masking [26][28] based countermeasures to further improve the SCA resistance.

7.5.7 Discussion

There are two aspects to the proposed countermeasure- 1) SCA resistance offered by a nominal digital LDO and 2) additional improvement with proposed SNI and R-VREF circuits in conjuction with ADCM. A nominal DLDO [Fig. 7.2] as discussed in Section II suppresses side channel leakage by attenuating small signal signatures and by adding large signal distortions. In our implementation, DLDO small signal behavior is dominated by the load pole and effectively acts as a LPF. This load pole is located at 16.7MHZ (I_L = 31mA, $V_{IN,DLDO}$ = 1V - ΔV_{PCB} = 1V - 31mA $\times$ 1Ω , V_{OUT} = 0.84V, V_{DO} = $V_{IN,DLDO}$ - V_{OUT}, $R_{power\text{-}stage}$ = V_{DO}/I_L = 4.16 Ω, C_L=2.3nF, F_L = 16.7MHz), where ΔV_{PCB} is the voltage drop across the 1Ω PCB resistor used for capturing power signatures). Since F_L is very small, high freq. signatures, specifically in the proximity of encryption clock frequency (F_{ENC}) are attenuated. Assuming 1st order system, a LPF with F_{3dB} of 16.7MHz has approximately 4.9$\times$ attenuation at 80MHz. This will lead to signal attenuation of 4.9$\times$ at 80MHz which in turn reduce SNR by the same amount. Since $MTD = \frac{1}{SNR^2}$ [99], we expect to see 24$\times$ increase in MTD due to small signal attenuation for frequencies in the proximity of the clock frequency, however, low frequency components which have been shown to be prominent leaking component with respect to SCA will not be affected by this attenuation. Therefore, small signal attenuation through digital LDO is not the primary reason for the increase in MTD [also demonstrated with respect to power gate and decoupling capacitance experiments in Section 5.4.1, Fig. 7.27, which essentially acts as a LPF comprising of decoupling capacitance (0.4nF or 2.3nF) and test-control switch resistance (2.36Ω) giving F_{3dB} of 169MHz or 29.3MHz for 0.4nF or 2.3nF decoupling capacitance]. Therefore, improvement in SCA resistance across the entire frequency spectrum for a nominal DLDO has to come from large signal distortions as described in Fig. 7.4(c).

SNI and R-VREF circuits when enabled with nominal DLDO improve the SCA resistance as demonstrated in previous sections. For SNI, we saw that increasing pulse width increases the amount of noise added and therefore reduces the SCA leakage. However,

when LFSR2 is used to increase the randomness by switching among 3 different pulse widths pseudo-randomly, the SCA leakage observed is more than with the highest possible pulse width. Therefore, we can surmise that pulse width is more important than its randomization. I'd like to note that some amount of randomness is already added as DLDO and encryption clocks are asynchronous. With SNI operated on DLDO clock, the relation between the location of SNI pulse with respect to encryption clock is already random. For R-VREF, the amount of randomness/noise added depends on the range of reference words (and therefore range of V_{ENC}). A higher range not only increases the noise added in the supply voltage but also increases the range of output clock frequencies generated by ADCM circuit. Since we are limited by the dynamic range of DLDO in the current testchip, the range of R-VREF in any future testchip should be designed to maximize the randomness added.

To break the proposed countermeasure, we not only needed to increase the number of measurements acquired to 10 million, we had to employ extensive filtering scheme utilizing narrow bandpass filters. Since we are using 31 bandpass filters (30 narrow and 1 wide) and are performing analysis in both time and frequency domains, we are spending approximately $2\times31 = 62\times$ more time on the analysis compared to a more traditional analysis method which only analyzes measurements in time domain using at most one bandpass filter centered around F_{ENC}. To reduce the analysis time, we can either run all the iterations in parallel using CPU clusters or employ a more efficient filtering scheme using a profiling step [137]. Moreover, more advanced attack methods such as template attacks [14], machine learning [145], deep learning [146, 147] can be employed to tackle poor SNR in the captured traces. Also, leakage models can be improved by using a linear regression method [148, 149] on the 8-bit power models for AES cores. Moreover, blind source separation can also be used to improve SNR in the measured signatures [150].

To remove the impact of frequency randomization, leakage power analysis (LPA) [136] can also be employed as a future work as LPA is only dependent on the current state of the

circuit in the steady state (when no operations are happening) and supply voltage but not dependent on the frequency of operation.

To improve the SCA resistance offered by proposed countermeasure, in addition to increasing the range of SNI and R-VREF, noise can directly be injected at $V_{IN,DLDO}$. The signatures that are captured at $V_{IN,DLDO}$ are already attenuated and a small amount of random noise can further suppress the available signal [81].

7.6 Summary

This chapter demonstrated enhanced power/EM SCA resistance of AES and SIMON encryption engines using a security-aware DLDO integrated with SNI & R-VREF circuits. With SCA analysis performed on power/EM signatures captured from a testchip fabricated in 130nm CMOS, we show that TVLA leakage is reduced by a factor of 25× for P-AES. Morever, CPA/CEMA analysis demonstrate that MTD for 80% SR increases by a factor of 3579×, 2182× and 500× for P-AES, S-AES and SIMON cores respectively at 10.4% performance, 32% power and 36.9% area overheads, indicating the generic and low-complexity nature of the proposed countermeasure.

CHAPTER 8
CONCLUSION AND FUTURE WORK

With modern computing devices taking over every aspect of human life, from high performance computing systems to billions of network-connected devices, energy-efficiency and security have become the biggest challenges to a address to ensure continued growth. This thesis investigates circuit techniques and architectures for improved energy-efficiency and SCA resistance for different cryptographic algorithms. Different datapath architectures for lightweight block cipher SIMON are developed and characterized with respect to ASIC and FPGA implementations to demonstrate energy-optimal and side channel resistant operation when the optimized SIMON engine is integrated with a low-power image sensor node. Since SCA resistance achieved with choice of datapath implementation is not sufficient, several lightweight SCA countermeasures utlilizing on-chip power management and low-power techniques are developed for 128-bit SIMON engine as well as for 128-bit AES cores. The detailed architecture for FIVR and DLDO integrated with ADCM circuit is presented to enable simultaneous supply and clock modulation for improved resistance against power, EM and fault based side channel attacks. Since all of these blocks are already integrated on-chip to facilitate fine-grained power management and error-free operation, they can also be leveraged to provide SCA resistance, using the techniques presented in this dissertation, making them an attractive option compared to most of the existing countermeasures. This chapter summarizes the main contributions in Section 8.1 and discusses future work and research directions in Section 8.2.

8.1 Dissertation Summary

We first establish the measurement and side channel analysis methodology in **Chapter 3**. Some of the commonly used metrics used for SCA methodology such as MTD for CPA

and CEMA analysis, SNR and t-statistic for TVLA analysis are described along with newly introduced correlation ratio (CR) and success rate (SR) metrics. Datapath architectures for 128-bit SIMON and 128-bit P-AES and S-AES cores used as encryption core prototype for FPGA and ASIC experiments in subsequent chapters are presented.

Chapter 4 highlights the need for lightweight cryptography in the context of IoT environment and how recently introduced lightweight cipher SIMON can address the challenges of resource constraints in these environments. Several datapath architectures for 128-bit SIMON at bit-level and round-level parallelism are implemented on ASIC using freePDK 15nm CMOS process and it is shown that 6-round unrolled datapath not only provides minimal energy operation (80$\times$ better) but also improves the SCA resistance by atleast 384$\times$ (characterized on Sakura-G FPGA board) while offering 143$\times$ increase in performance compared to bitserial implementation, demonstrating that bitserial datapaths, even though the most compact, are not optimal when other important tradeoffs such as energy, performance and SCA resistance are considered. Application of optimized SIMON architectures to a low-power image sensor node shows negligible overheads associated with integrating SCA hardened encryption engine with the IoT edge node facilitating both mathematical and side channel security.

Different datapath architectures are susceptible to side channel attacks to a different degree with parallel and round-unrolled datapaths due to algorithmic noise have reduced information leakage compared to serialized datapaths as demonstrated for SIMON in previous chapter and also true for hardware implementations of AES. However, the improvement in SCA resistance inherent to datapath implementation is not sufficient and dedicated countermeasures are required to further harden the encryption cores. Subsequent chapters discuss several circuit techniques that leverage on-chip power management and employ additional hiding or randomization circuits to further improve physical side channel defenses.

Chapter 5 describes Random Fast Voltage Dithering (RFVD) scheme developed using on-chip integrated FIVR and ADCM circuit to provide SCA resistance for 128-bit AES

cores at their local supply node (V_{AES}). With RFVD, both power and EM signatures are scrambled owing to 1) 6 different randomized operating conditions (voltage and frequency - V-F) across encryptions, 2) local modulator (LM) inducing randomness with random clock gating and duty modulation, 3) global modulator based frequency randomization (GM-FR) and 4) FIVR loop randomizer (LR) adding randomness at V_{AES}. Proposed randomization schemes randomize both amplitude and timing of signals in side channel signatures and result in misalignment of time samples and reduced SNR leading to increase in SCA resistance. The P-SCA measurements taken from 130nm CMOS testchip prototype demonstrate reduction of upto 37.3$\times$ in TVLA leakage and increase of 642$\times$ in CPA MTD. Since proposed techniques scramble both power/EM signatures, similar resistance is observed for SCA hardened design with respect to P-SCA and EM-SCA.

Since ADCM circuit enables error-free operation in presence of supply fluctuations or process or temperature variations, it can be used to protect against supply glitch or temperate variations induced faults. **Chapter 6** develops a simple measurement setup, by integrating testchip prototype and Sakura-G FPGA board, to inject supply glitch or temperature fluctuation related faults during encryption operation for S-AES core. A successful fault injection attack is demonstrated for unprotected (standalone) S-AES core under different settings for induced supply glitches. For protected S-AES core (S-AES+ADCM), we can no longer inject these faults even with 10 million encryptions indicating usefulness of ADCM to mitigate fault injection attacks.

Due to high design complexity and silicon area for FIVR, RFVD scheme that was proposed in Chapter 5 may not be suitable for ultra-lightweight IoT edge devices. To address this, lightweight SCA countermeasures utilizing digital LDO and ADCM circuits are developed in **Chapter 7**. Different transformations that are induced through DLDO into power signatures before they are measured at the input supply node of the chip ($V_{IN,DLDO}$) are discussed. Small signal attenuation and large signal distortions are shown to be major contributors to information loss. However, a nominal DLDO provides only a limited

improvement and two circuit techniques, namely switching noise injector (SNI) and Random VREF generator (R-VREF) are presented to further improve the SCA resistance. A testchip prototype containing these circuits, AES and SIMON cores is developed in 130nm CMOS and measured results demonstrate improved SCA resistance (in terms of MTD for 80% SR) by a factor of 3579×, 2182× and 500× for P-AES, S-AES and SIMON cores respectively with respect to both P-SCA and EM-SCA. The design overheads associated with proposed hardening circuits are 10.4% performance, 32% power and 36.9% area indicating their generic and low-complexity nature. In summary, we demonstrate that a security-aware digital LDO can not only provide point of load regulation but also facilitate point of load side channel security.

8.2 Future Directions

Since power and EM based side channels are created due to sudden current drawn by the digital circuits, techniques to lower power consumption affect side channel characteristics. Therefore, power-management and low-power circuit techniques which are already employed on-chip for distributed power management systems can be leveraged to improve SCA resistance facilitating energy-efficient and secure computing as demonstrated by this thesis and some other recently published work [48, 60, 81, 151].

8.2.1 Energy, Security and Performance Tradeoffs

Even though the proposed circuits suppress information leakage, tradeoffs among energy, security and performance are inherent. A high bandwidth FIVR/DLDO can provide better DVFS management therefore improving performance or reducing energy but it may lead to higher information leakage as high frequency signal in the encryption signatures pass through FIVR/DLDO without significant attenuation. For the proposed R-VREF circuit, correct clock edges are generated even during the supply voltage transitions and encryption engine operates normally. A faster transition means supply voltage is at a number of fixed

levels (depending on the number of reference words) most of the time generating a number of fixed frequency levels. However, a slower transition means higher number of frequency levels generated corresponding to instantaneous voltage during the transition. The number of generated frequency levels depend not only on the range of the transition but also the speed or slew rate. Therefore, a smaller bandwidth FIVR/DLDO may potentially improve the SCA resistance by not only only suppressing the high frequency side channel signatures but also by increasing the number of instantaneous V-F pairs generated. On the other hand, a high bandwidth DLDO may be better for leakage suppression with respect to SNI as DLDO quickly responds to noise events as a result of SNI generating more noise. The interaction between SNI, R-VREF and DLDO parameters (bandwidth and phase margin) is complex and has to be carefully analyzed/measured to improve the proposed countermeasures for higher SCA resistance.

8.2.2 Compute Complexity and Ideas to Improve Proposed Techniques

While quantifying the improvement in side channel leakage, we employed extensive filtering techniques with upto 100 filter bands for RFVD and upto 30 filter bands for DLDO with SNI & R-VREF countermeasures. Traditionally, only one or no filter band is employed for filtering. Therefore, with our postprocessing methods, the analysis time increases by a factor of 100$\times$ or 30 $\times$ for RFVD and DLDO with SNI & R-VREF respectively. Even though this increased analysis time is not included in the MTD metric, it will significantly increase the difficulty to recover the secret key with respect to increased time or compute and memory complexity. To reduce filter bands, we can use a profiling step first to figure out the most leaking band and then use that to recover the secret key for unknown devices.

Proposed techniques, including RFVD with FIVR & ADCM and SNI/R-VREF with DLDO & ADCM, essentially rely on randomization of signatures. However, this randomization is achieved using pseudorandom number generators implemented on-chip using LFSR. Since LFSR follows a deterministic pattern, it may be possible to detect the LFSR

pattern using pattern matching/detection techniques. Another drawback is the range of LFSR. We are using 2-5 bit LFSRs which have limited randomization range. By increasing the range, it may be possible to increase the extent of signal randomization, especially for R-VREF where increased number of reference words will increase the number and range of supply and frequency levels generated. Similarly, by increasing the width of SNI pulse out, we can disconnect the leakage path from V_{ENC} to $V_{IN,DLDO}$ for longer fraction of DLDO clock cycle. We may need to increase the load capacitor (C_L) to contain the injected noise within some pre-determined level.

8.2.3 Advanced Power Models and Attack Methods

Traditional hamming distance (HD) or hamming weight (HW) based power models only model the switching activity at the intermediate nodes. They don't model the other parts of the power consumption - supply, frequency and intermediate node capacitances as these are assumed to be fixed throughout the experiment. With the proposed techniques, the assumption about intermediate node capacitance is still correct, however, supply voltage and frequency vary during the experiment, in fact, from encryption to encryption and even during the same encryption. Therefore, a better hypothetical power model would model both of these for increased accuracy, especially for DVFS or DVS based countermeasures [44, 82]. However, since, voltage and frequency are changed randomly across different and even during the same encryptions in this work, it may not be possible to know supply and frequency of operation.

Since proposed countermeasures add amplitude and timing noise leading to reduced SNR, techniques to improve SNR can be employed to improve attack results. Filtering schemes and frequency domain attacks try to achieve this to some extent but better methods such as blind source separation [152] or linear regression [153] based statistical methods can be used to improve SNR. Additionally, higher order attacks, such as template attacks [14] or machine learning/deep learning [146, 154] attacks can potentially reduce

the number of measurements required to recover the correct key. However, some of these techniques are not robust to increased noise in the captured signatures so the proposed countermeasure are expected to perform well.

8.2.4 Application to Other Cryptographic Algorithms

Application of the proposed countermeasures to other cryptographic algorithms, especially public key cryptographic alogirhtms, may not have the same impact as demonstrated for SIMON and AES cores. Compared to symmetric key encryption schemes, public key encryption schemes, suchs as RSA and ECC run for 100s of thousands of cycles and leak signatures over a longer period (side channel leakage in low-frequency bands). The proposed DLDO has a bandwidth of $\sim$10MHz indicating sub-10MHz signals will not have any small signal attenuation at all. Therefore, a nominal DLDO may not affect the side channel leakage of these algorithms significantly. However, the proposed SNI and R-VREF circuits add both high-frequency and low-frequency noise and more importantly, the asynchronous relation between DLDO clock and encryption clock adds timing noise which will help in providing SCA resistance for public key encryption algorithms too.

Appendices

APPENDIX A

ABBREVIATIONS

ADC	Analog-to-Digital Converter
ADCM	All Digital Clock Modulation
AES	Advanced Encryption Standard
B-RFVD	Basic Random Fast Voltage Dithering
CPA	Correlation Power Analysis
CEMA	Correlation ElectroMagnetic Analysis
CR	Correlation Ratio
DLDO	Digital Low Drop-Out
DPA	Differential Power Analysis
DPID	Digital Proportional-Integral-Derivative
EM-SCA	ElectroMagnetic Side-Channel-Attack
FA	Fault Attack
FFT	Fast Fourier Transform
FIA	Fault Injection Attack
FIVR	Fully Integrated Inductive Voltage Regulator
GM	Global Modulator
GM-FR	Global Modulator based Frequency Randomization
HD	Hamming Distance
HW	Hamming Weight
I-RFVD	Improved Random Fast Voltage Dithering
IoT	Internet of Things
IVR	Integrated Voltage Regulator

LCO Limit Cycle Oscillation

LDO Low Dropout Regulator

LM Local Modulator

LPF Low Pass Filter

LR Loop Randomization (Randomizer)

MTD Minimum-Traces-to-Disclose

P-AES Parallel AES

P-SCA Power Side-Channel-Attack

PID Proportional-Integral-Derivative

PM Phase-Margin

R-VREF Randomized VREF Generator

RFVD Random Fast Voltage Dithering

RTA Resistive-Transient-Assist

S-AES Serial AES

SCVR Switched-Capacitor based Voltage Regulator

SCA Side Channel Attack

SNI Switching Noise Injector

SNR Signal to Noise Ratio

SR Success Rate

TA Template Attack

TVLA Test Vector Leakage Assessment

UGF Unity-Gain-Bandwidth

VR(M) Voltage Regulator (Module)

REFERENCES

[1] Jayavardhana Gubbi et al. “Internet of Things (IoT): A vision, architectural elements, and future directions”. In: *Future Generation Computer Systems* 29.7 (2013). Including Special sections: Cyber-enabled Distributed Computing for Ubiquitous Cloud and Network Services & Cloud Computing and Scientific Applications Big Data, Scalable Analytics, and Beyond, pp. 1645 –1660.

[2] A. Zanella et al. “Internet of Things for Smart Cities”. In: *IEEE Internet of Things Journal* 1.1 (2014), pp. 22–32.

[3] Rolf H. Weber. “Internet of Things New security and privacy challenges”. In: *Computer Law & Security Review* 26.1 (2010), pp. 23 –30.

[4] Paul C. Kocher. “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”. In: *Advances in Cryptology — CRYPTO ’96*. Ed. by Neal Koblitz. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104–113. ISBN: 978-3-540-68697-2.

[5] Dakshi Agrawal et al. “The EM Side—Channel(s)”. In: *Cryptographic Hardware and Embedded Systems - CHES 2002*. Ed. by Burton S. Kaliski, çetin K. Koç, and Christof Paar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45. ISBN: 978-3-540-36400-9.

[6] Peng Cheng et al. “SonarSnoop: Active Acoustic Side-Channel Attacks”. In: *CoRR* abs/1808.10250 (2018). arXiv: 1808.10250.

[7] Paul Kocher et al. “Spectre Attacks: Exploiting Speculative Execution”. In: *40th IEEE Symposium on Security and Privacy (S&P’19)*. 2019.

[8] Moritz Lipp et al. “Meltdown: Reading Kernel Memory from User Space”. In: *27th USENIX Security Symposium (USENIX Security 18)*. 2018.

[9] Michael Schwarz et al. “ZombieLoad: Cross-Privilege-Boundary Data Sampling”. In: *arXiv:1905.05726* (2019).

[10] F. Liu et al. “Last-Level Cache Side-Channel Attacks are Practical”. In: *2015 IEEE Symposium on Security and Privacy*. 2015, pp. 605–622.

[11] Galen Hunt, George Letey, and Ed Nightingale. *The Seven Properties of Highly Secure Devices*. Tech. rep. MSR-TR-2017-16. 2017.

[12] Paul Kocher, Joshua Jaffe, and Benjamin Jun. “Differential Power Analysis”. In: *Advances in Cryptology — CRYPTO’ 99*. Ed. by Michael Wiener. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397. ISBN: 978-3-540-48405-9.

[13] Eric Brier, Christophe Clavier, and Francis Olivier. “Correlation Power Analysis with a Leakage Model”. In: *Cryptographic Hardware and Embedded Systems - CHES 2004*. Ed. by Marc Joye and Jean-Jacques Quisquater. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 16–29. ISBN: 978-3-540-28632-5.

[14] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. “Template Attacks”. In: *Cryptographic Hardware and Embedded Systems - CHES 2002*. Ed. by Burton S. Kaliski, çetin K. Koç, and Christof Paar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 13–28. ISBN: 978-3-540-36400-9.

[15] Bo Yu et al. “An AES chip with DPA resistance using hardware-based random order execution”. In: *Journal of Semiconductors* 33.6 (2012), p. 065009.

[16] Jude Angelo Ambrose, Sri Parameswaran, and Aleksandar 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*. ICCAD ’08. San Jose, California: IEEE Press, 2008, pp. 678–684. ISBN: 978-1-4244-2820-5.

[17] Felipe Ghellar and Marcelo S. Lubaszewski. “A Novel AES Cryptographic Core Highly Resistant to Differential Power Analysis Attacks”. In: *Proceedings of the 21st Annual Symposium on Integrated Circuits and System Design*. SBCCI ’08. Gramado, Brazil: ACM, 2008, pp. 140–145. ISBN: 978-1-60558-231-3.

[18] J. 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*. 2010, pp. 273–280.

[19] Thomas Popp et al. “Evaluation of the Masked Logic Style MDPL on a Prototype Chip”. In: *Cryptographic Hardware and Embedded Systems - CHES 2007*. Ed. by Pascal Paillier and Ingrid Verbauwhede. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 81–94. ISBN: 978-3-540-74735-2.

[20] E. Amouri et al. “Balancing WDDL dual-rail logic in a tree-based FPGA to enhance physical security”. In: *2014 24th International Conference on Field Programmable Logic and Applications (FPL)*. 2014, pp. 1–4.

[21] C. Tokunaga and D. Blaauw. “Secure AES engine with a local switched-capacitor current equalizer”. In: *2009 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*. 2009, 64–65,65a.

[22] R. Menicocci, A. Trifiletti, and F. Trotta. “Experiments on two clock countermeasures against power analysis attacks”. In: *2014 Proceedings of the 21st International Conference Mixed Design of Integrated Circuits and Systems (MIXDES)*. 2014, pp. 215–219.

[23] Daisuke Suzuki and Minoru Saeki. “Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style”. In: *Cryptographic Hardware and Embedded Systems - CHES 2006*. Ed. by Louis Goubin and Mitsuru Matsui. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 255–269. ISBN: 978-3-540-46561-4.

[24] M. Nassar et al. “BCDL: A high speed balanced DPL for FPGA with global precharge and no early evaluation”. In: *2010 Design, Automation Test in Europe Conference Exhibition (DATE 2010)*. 2010, pp. 849–854.

[25] Marco Bucci et al. “Three-Phase Dual-Rail Pre-charge Logic”. In: *Cryptographic Hardware and Embedded Systems - CHES 2006*. Ed. by Louis Goubin and Mitsuru Matsui. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 232–241. ISBN: 978-3-540-46561-4.

[26] Stefan Mangard, Norbert Pramstaller, and Elisabeth Oswald. “Successfully Attacking Masked AES Hardware Implementations”. In: *Cryptographic Hardware and Embedded Systems – CHES 2005*. Ed. by Josyula R. Rao and Berk Sunar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 157–171. ISBN: 978-3-540-31940-5.

[27] M. Doulcier-Verdier et al. “A side-channel and fault-attack resistant AES circuit working on duplicated complemented values”. In: *2011 IEEE International Solid-State Circuits Conference*. 2011, pp. 274–276.

[28] Begül Bilgin et al. “Higher-Order Threshold Implementations”. In: *Advances in Cryptology – ASIACRYPT 2014*. Ed. by Palash Sarkar and Tetsu Iwata. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 326–343. ISBN: 978-3-662-45608-8.

[29] S. Lu, Z. Zhang, and M. Papaefthymiou. “1.32GHz high-throughput charge-recovery AES core with resistance to DPA attacks”. In: *2015 Symposium on VLSI Circuits (VLSI Circuits)*. 2015, pp. C246–C247.

[30] Julia Borghoff et al. “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”. In: *Advances in Cryptology – ASIACRYPT 2012*. Ed. by Xiaoyun Wang and Kazue Sako. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 208–225. ISBN: 978-3-642-34961-4.

[31] A. Bogdanov et al. “PRESENT: An Ultra-Lightweight Block Cipher”. In: *Cryptographic Hardware and Embedded Systems - CHES 2007*. Ed. by Pascal Paillier and Ingrid Verbauwhede. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466. ISBN: 978-3-540-74735-2.

[32] P. Proenca and R. Chaves. “Compact CLEFIA Implementation on FPGAS”. In: *2011 21st International Conference on Field Programmable Logic and Applications*. 2011, pp. 512–517.

[33] Guido Bertoni et al. “Keccak”. In: *Advances in Cryptology – EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 313–314. ISBN: 978-3-642-38348-9.

[34] [18] P. Barreto et. al. *The WHIRLPOOL hash function*. White Paper. `www.larc.usp.br/~pbarreto/WhirlpoolPage.html`.

[35] R. Beaulieu et al. “The SIMON and SPECK lightweight block ciphers”. In: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*. 2015, pp. 1–6.

[36] A. Aysu, E. Gulcan, and P. Schaumont. “SIMON Says: Break Area Records of Block Ciphers on FPGAs”. In: *IEEE Embedded Systems Letters* 6.2 (2014), pp. 37–40.

[37] Padmanabhan Pillai and Kang G. Shin. “Real-time Dynamic Voltage Scaling for Low-power Embedded Operating Systems”. In: *SIGOPS Oper. Syst. Rev.* 35.5 (Oct. 2001), pp. 89–102.

[38] G. Semeraro et al. “Energy-efficient processor design using multiple clock domains with dynamic voltage and frequency scaling”. In: *Proceedings Eighth International Symposium on High Performance Computer Architecture*. 2002, pp. 29–40.

[39] N. Kurd et al. “5.9 Haswell: A family of IA 22nm processors”. In: *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*. 2014, pp. 112–113.

[40] Z. Toprak-Deniz et al. “5.2 Distributed system of digitally controlled microregulators enabling per-core DVFS for the POWER8TMmicroprocessor”. In: *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*. 2014, pp. 98–99.

[41] T. Singh et al. “3.2 Zen: A next-generation high-performance 86 core”. In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, pp. 52–53.

[42] K. Chae and S. Mukhopadhyay. “All-Digital Adaptive Clocking to Tolerate Transient Supply Noise in a Low-Voltage Operation”. In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 59.12 (2012), pp. 893–897.

[43] M. S. Floyd et al. “26.5 Adaptive clocking in the POWER9 processor for voltage droop protection”. In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, pp. 444–445.

[44] Shengqi Yang et al. “Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach”. In: *Design, Automation and Test in Europe*. 2005, 64–69 Vol. 3.

[45] K. Baddam and M. Zwolinski. “Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure”. In: *20th International Conference on VLSI Design held jointly with 6th International Conference on Embedded Systems (VLSID’07)*. 2007, pp. 854–862.

[46] M. Kar et al. “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)*. 2017, pp. 142–143.

[47] V. Telandro et al. “On-Chip Voltage Regulator Protecting Against Power Analysis Attacks”. In: *2006 49th IEEE International Midwest Symposium on Circuits and Systems*. Vol. 2. 2006, pp. 507–511.

[48] O. A. Uzun and S. Kse. “Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System”. In: *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* 4.2 (2014), pp. 169–179.

[49] M. Kar et al. “Impact of inductive integrated voltage regulator on the power attack vulnerability of encryption engines: A simulation study”. In: *Proceedings of the IEEE 2014 Custom Integrated Circuits Conference*. 2014, pp. 1–4.

[50] Monodeep Kar et al. “Exploiting Fully Integrated Inductive Voltage Regulators to Improve Side Channel Resistance of Encryption Engines”. In: *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*. ISLPED ’16. San Francisco Airport, CA, USA: ACM, 2016, pp. 130–135. ISBN: 978-1-4503-4185-1.

[51] M. Kar et al. “Invited paper: Low power requirements and side-channel protection of encryption engines: Challenges and opportunities”. In: *2017 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. 2017, pp. 1–2.

[52] M. Kar et al. “What does ultra low power requirements mean for side-channel secure cryptography?” In: *2016 IEEE 34th International Conference on Computer Design (ICCD)*. 2016, pp. 686–689.

[53] D. Das et al. “High efficiency power side-channel attack immunity using noise injection in attenuated signature domain”. In: *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2017, pp. 62–67.

[54] S. Mathew et al. “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”. In: *IEEE Journal of Solid-State Circuits* 50.4 (2015), pp. 1048–1058.

[55] Amir Moradi et al. “Pushing the Limits: A Very Compact and a Threshold Implementation of AES”. In: *Advances in Cryptology – EUROCRYPT 2011*. Ed. by Kenneth G. Paterson. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 69–88. ISBN: 978-3-642-20465-4.

[56] N. Ahmad and S. M. R. Hasan. “Efficient integrated AES crypto-processor architecture for 8-bit stream cipher”. In: *Electronics Letters* 48.23 (2012), pp. 1456–1457.

[57] Zhigang Hu et al. “Microarchitectural techniques for power gating of execution units”. In: *Proceedings of the 2004 International Symposium on Low Power Electronics and Design (IEEE Cat. No.04TH8758)*. 2004, pp. 32–37.

[58] Vivek Tiwari et al. “Reducing Power in High-performance Microprocessors”. In: *Proceedings of the 35th Annual Design Automation Conference*. DAC ’98. San Francisco, California, USA: ACM, 1998, pp. 732–737. ISBN: 0-89791-964-5.

[59] N. Sturcken et al. “A 2.5D Integrated Voltage Regulator Using Coupled-Magnetic-Core Inductors on Silicon Interposer”. In: *IEEE Journal of Solid-State Circuits* 48.1 (2013), pp. 244–254.

[60] M. Kar et al. “An All-Digital Fully Integrated Inductive Buck Regulator With A 250-MHz Multi-Sampled Compensator and a Lightweight Auto-Tuner in 130-nm CMOS”. In: *IEEE Journal of Solid-State Circuits* 52.7 (2017), pp. 1825–1835.

[61] V. C. K. Chekuri et al. “Autotuning of Integrated Inductive Voltage Regulator Using On-Chip Delay Sensor to Tolerate Process and Passive Variations”. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2019), pp. 1–11.

[62] V. C. K. Chekuri et al. “Performance based tuning of an inductive integrated voltage regulator driving a digital core against process and passive variations”. In: *2018*

Design, Automation Test in Europe Conference Exhibition (DATE). 2018, pp. 367–372.

[63] S. B. Nasir, S. Gangopadhyay, and A. Raychowdhury. "All-Digital Low-Dropout Regulator With Adaptive Control and Reduced Dynamic Stability for Digital Load Circuits". In: *IEEE Transactions on Power Electronics* 31.12 (2016), pp. 8293–8302.

[64] X. Ma et al. "A 0.4V 430nA quiescent current NMOS digital LDO with NAND-based analog-assisted loop in 28nm CMOS". In: *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*. 2018, pp. 306–308.

[65] M. Huang et al. "20.4 An output-capacitor-free analog-assisted digital low-dropout regulator with tri-loop control". In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, pp. 342–343.

[66] W. Tsou et al. "20.2 Digital low-dropout regulator with anti PVT-variation technique for dynamic voltage scaling and adaptive voltage scaling multicore processor". In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2017, pp. 338–339.

[67] A. Singh et al. "A Digital Low-Dropout Regulator with Auto-Tuned PID Compensator and Dynamic Gain Control for Improved Transient Performance under Process Variations and Aging". In: *accepted for publications in IEEE Transactions on Power Electronics* (2019).

[68] V. C. Krishna Chekuri et al. "On the Effect of NBTI Induced Aging of Power Stage on the Transient Performance of On-Chip Voltage Regulators". In: *2019 IEEE International Reliability Physics Symposium (IRPS)*. 2019, pp. 1–5.

[69] A. Drake et al. "A Distributed Critical-Path Timing Monitor for a 65nm High-Performance Microprocessor". In: *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*. 2007, pp. 398–399.

[70] A. Grenat et al. "5.6 Adaptive clocking system for improved power efficiency in a 28nm x86-64 microprocessor". In: *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*. 2014, pp. 106–107.

[71] K. A. Bowman et al. "A 22 nm All-Digital Dynamically Adaptive Clock Distribution for Supply Voltage Droop Tolerance". In: *IEEE Journal of Solid-State Circuits* 48.4 (2013), pp. 907–916.

[72] D. Ernst et al. "Razor: a low-power pipeline based on circuit-level timing speculation". In: *Proceedings. 36th Annual IEEE/ACM International Symposium on Microarchitecture, 2003. MICRO-36.* 2003, pp. 7–18.

[73] D. Blaauw et al. “Razor II: In Situ Error Detection and Correction for PVT and SER Tolerance”. In: *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*. 2008, pp. 400–622.

[74] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. “On the Importance of Checking Cryptographic Protocols for Faults”. In: *Advances in Cryptology — EUROCRYPT ’97*. Ed. by Walter Fumy. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 37–51. ISBN: 978-3-540-69053-5.

[75] Edgar Mateos and Catherine H. Gebotys. “A New Correlation Frequency Analysis of the Side Channel”. In: *Proceedings of the 5th Workshop on Embedded Systems Security*. WESS ’10. Scottsdale, Arizona: ACM, 2010, 4:1–4:8. ISBN: 978-1-4503-0078-0.

[76] B. J. Gilbert Goodwill, J. Jaffe, and P. Rohatgi. “A testing methodology for side-channel resistance validation”. In: *NIST Non-invasive Attack Testing Workshop*.

[77] T. Popp, S. Mangard, and E. Oswald. “Power Analysis Attacks and Countermeasures”. In: *IEEE Design Test of Computers* 24.6 (2007), pp. 535–543.

[78] Xinmu Wang et al. “Role of power grid in side channel attack and power-grid-aware secure design”. In: *2013 50th ACM/EDAC/IEEE Design Automation Conference (DAC)*. 2013, pp. 1–9.

[79] Matthieu Rivain and Emmanuel Prouff. “Provably Secure Higher-Order Masking of AES”. In: *Cryptographic Hardware and Embedded Systems, CHES 2010*. Ed. by Stefan Mangard and François-Xavier Standaert. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 413–427. ISBN: 978-3-642-15031-9.

[80] HeeSeok Kim, Seokhie Hong, and Jongin Lim. “A Fast and Provably Secure Higher-Order Masking of AES S-Box”. In: *Cryptographic Hardware and Embedded Systems – CHES 2011*. Ed. by Bart Preneel and Tsuyoshi Takagi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 95–107. ISBN: 978-3-642-23951-9.

[81] D. Das et al. “ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity”. In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 65.10 (2018), pp. 3300–3311.

[82] Roman Korkikian, David Naccache, and Guilherme Ozari de Almeida. *Instantaneous Frequency Analysis*. Cryptology ePrint Archive, Report 2013/320. `https://eprint.iacr.org/2013/320`. 2013.

[83] A. Singh et al. “Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators”. In: *2015 IEEE/ACM In-*

ternational Symposium on Low Power Electronics and Design (ISLPED). 2015, pp. 134–139.

[84] A. Singh et al. "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)*. 2016, pp. 145–148.

[85] Arvind Singh et al. "Reducing Side-Channel Leakage of Encryption Engines Using Integrated Low-Dropout Voltage Regulators". In: *Journal of Hardware and Systems Security* 1.4 (2017), pp. 340–355.

[86] Debayan Das et al. *STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis*. Cryptology ePrint Archive, Report 2018/620. `https://eprint.iacr.org/2018/620`. 2018.

[87] Eli Biham and Adi Shamir. "Differential fault analysis of secret key cryptosystems". In: *Advances in Cryptology — CRYPTO '97*. Ed. by Burton S. Kaliski. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 513–525. ISBN: 978-3-540-69528-8.

[88] Christophe Giraud. "DFA on AES". In: *Advanced Encryption Standard – AES*. Ed. by Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 27–41. ISBN: 978-3-540-31840-8.

[89] Gilles Piret and Jean-Jacques Quisquater. "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and Khazad". In: *Cryptographic Hardware and Embedded Systems - CHES 2003*. Ed. by Colin D. Walter, Çetin K. Koç, and Christof Paar. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 77–88. ISBN: 978-3-540-45238-6.

[90] T. Fukunaga and J. Takahashi. "Practical Fault Attack on a Cryptographic LSI with ISO/IEC 18033-3 Block Ciphers". In: *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. 2009, pp. 84–92.

[91] Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo. "CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management". In: *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017, pp. 1057–1074. ISBN: 978-1-931971-40-9.

[92] A. Barenghi et al. "Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures". In: *Proceedings of the IEEE* 100.11 (2012), pp. 3056–3076.

[93] Chih-Hsu Yen and Bing-Fei Wu. “Simple error detection methods for hardware implementation of Advanced Encryption Standard”. In: *IEEE Transactions on Computers* 55.6 (2006), pp. 720–731.

[94] B. Wang et al. “Exploration of Benes Network in Cryptographic Processors: A Random Infection Countermeasure for Block Ciphers Against Fault Attacks”. In: *IEEE Transactions on Information Forensics and Security* 12.2 (2017), pp. 309–322.

[95] Kamil Gomina et al. “Detecting Positive Voltage Attacks on CMOS Circuits”. In: *Proceedings of the First Workshop on Cryptography and Security in Computing Systems*. CS2 ’14. Vienna, Austria: ACM, 2014, pp. 1–6. ISBN: 978-1-4503-2484-7.

[96] K. Gomina et al. “Power supply glitch attacks: Design and evaluation of detection circuits”. In: *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 2014, pp. 136–141.

[97] L. Zussa et al. “Efficiency of a glitch detector against electromagnetic fault injection”. In: *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2014, pp. 1–6.

[98] EMC Probes. “Accessed: Feb. 19, 2018. Available: https://www.beehive-electronics.com/datasheets/100SeriesDatasheetCurrent.pdf”. In: *Online*.

[99] Y. Souissi L. Sauvage S. Guilley H. Maghrebi and J.-L. Danger. “Quantifying the quality of side channel acquisitions”. In: *2017 IEEE International Solid-State Circuits Conference (ISSCC)*. 2011.

[100] A. Singh et al. “Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering”. In: *IEEE Journal of Solid-State Circuits* 54.2 (2019), pp. 569–583.

[101] A. Singh et al. “Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-Edge Nodes”. In: *IEEE Internet of Things Journal* 6.1 (2019), pp. 421–434.

[102] Akashi Satoh et al. “A Compact Rijndael Hardware Architecture with S-Box Optimization”. In: *Advances in Cryptology — ASIACRYPT 2001*. Ed. by Colin Boyd. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 239–254. ISBN: 978-3-540-45682-7.

[103] A. Singh et al. “Energy efficient and side-channel secure hardware architecture for lightweight cipher SIMON”. In: *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2018, pp. 159–162.

[104] P. Yalla and J. Kaps. “Lightweight Cryptography for FPGAs”. In: *2009 International Conference on Reconfigurable Computing and FPGAs*. 2009, pp. 225–230.

[105] Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević. “KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers”. In: *Cryptographic Hardware and Embedded Systems - CHES 2009*. Ed. by Christophe Clavier and Kris Gaj. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 272–288. ISBN: 978-3-642-04138-9.

[106] Toru Akishita and Harunaga Hiwatari. “Very Compact Hardware Implementations of the Blockcipher CLEFIA”. In: *Selected Areas in Cryptography*. Ed. by Ali Miri and Serge Vaudenay. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 278–292. ISBN: 978-3-642-28496-0.

[107] Kazumaro Aoki et al. “Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms — Design andAnalysis”. In: *Selected Areas in Cryptography*. Ed. by Douglas R. Stinson and Stafford Tavares. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 39–56. ISBN: 978-3-540-44983-6.

[108] Pieter Maene and Ingrid Verbauwhede. “Single-Cycle Implementations of Block Ciphers”. In: *Revised Selected Papers of the 4th International Workshop on Lightweight Cryptography for Security and Privacy - Volume 9542*. LightSec 2015. Bochum, Germany: Springer-Verlag, 2016, pp. 131–147. ISBN: 978-3-319-29077-5.

[109] Subhadeep Banik et al. *Midori: A Block Cipher for Low Energy (Extended Version)*. Cryptology ePrint Archive, Report 2015/1142. `https://eprint.iacr.org/2015/1142`. 2015.

[110] Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni. “Exploring Energy Efficiency of Lightweight Block Ciphers”. In: *Revised Selected Papers of the 22Nd International Conference on Selected Areas in Cryptography - SAC 2015 - Volume 9566*. Berlin, Heidelberg: Springer-Verlag, 2016, pp. 178–194. ISBN: 978-3-319-31300-9.

[111] Lejla Batina et al. “Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures”. In: *Radio Frequency Identification*. Ed. by Michael Hutter and Jörn-Marc Schmidt. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 103–112. ISBN: 978-3-642-41332-2.

[112] Axel Poschmann et al. “A Family of Light-Weight Block Ciphers Based on DES Suited For RFID Applications”. In: *PROCEEDINGS OF FSE 2007, LNCS*. Springer-Verlag, 2006.

[113] Begül Bilgin et al. “Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware”. In: *Cryptographic Hardware and Embedded Systems - CHES 2013*. Ed. by Guido Bertoni and Jean-Sébastien Coron. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 142–158. ISBN: 978-3-642-40349-1.

[114] Amir Moradi and Axel Poschmann. “Lightweight Cryptography and DPA Countermeasures: A Survey”. In: *Financial Cryptography and Data Security*. Ed. by Radu Sion et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 68–79. ISBN: 978-3-642-14992-4.

[115] Ege Gulcan, Aydin Aysu, and Patrick Schaumont. “A Flexible and Compact Hardware Architecture for the SIMON Block Cipher”. In: *Lightweight Cryptography for Security and Privacy*. Ed. by Thomas Eisenbarth and Erdinç Öztürk. Cham: Springer International Publishing, 2015, pp. 34–50. ISBN: 978-3-319-16363-5.

[116] Jos Wetzels and Wouter Bokslag. *Simple SIMON: FPGA implementations of the SIMON 64/128 Block Cipher*. Cryptology ePrint Archive, Report 2016/029. `https://eprint.iacr.org/2016/029`. 2016.

[117] S. Bhasin et al. “A look into SIMON from a side-channel perspective”. In: *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. 2014, pp. 56–59.

[118] Dillibabu Shanmugam, Ravikumar Selvam, and Suganya Annadurai. “Differential Power Analysis Attack on SIMON and LED Block Ciphers”. In: *Security, Privacy, and Applied Cryptography Engineering*. Ed. by Rajat Subhra Chakraborty, Vashek Matyas, and Patrick Schaumont. Cham: Springer International Publishing, 2014, pp. 110–125. ISBN: 978-3-319-12060-7.

[119] *Opencores*. `http://opencores.org/`.

[120] Shivam Bhasin et al. “Unrolling Cryptographic Circuits: A Simple Countermeasure Against Side-Channel Attacks”. In: *Topics in Cryptology - CT-RSA 2010*. Ed. by Josef Pieprzyk. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 195–207. ISBN: 978-3-642-11925-5.

[121] L. Loder et al. “Towards a framework to perform DPA attack on GALS pipeline architectures”. In: *2014 27th Symposium on Integrated Circuits and Systems Design (SBCCI)*. 2014, pp. 1–7.

[122] F. Conti et al. “An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics”. In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 64.9 (2017), pp. 2481–2494.

[123] G. Hofemeier and R. Chesebrough. *Introduction to Intel AES-NI and Intel secure key instructions*. White Paper. https://software.intel.com/en-us/articles/introduction-to-intel-aes-ni-and-intel-secure-key-instructions. 2012.

[124] J. Powell D. Kaplan and T. Woller. *Secure Memory Encryption (SME) - x86*. White Paper. https://en.wikichip.org/wiki/x86/sme. 2016.

[125] J. H. Ko, T. Na, and S. Mukhopadhyay. "An energy-efficient wireless video sensor node with a region-of-interest based multi-parameter rate controller for moving object surveillance". In: *2016 13th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. 2016, pp. 138–144.

[126] Jong Hwan Ko and Saibal Mukhopadhyay. "An Energy-Aware Approach to Noise-Robust Moving Object Detection for Low-Power Wireless Image Sensor Platforms". In: *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*. ISLPED '16. San Francisco Airport, CA, USA: ACM, 2016, pp. 194–199. ISBN: 978-1-4503-4185-1.

[127] A. Singh et al. "Exploiting on-chip power management for side-channel security". In: *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2018, pp. 401–406.

[128] M. Kar et al. "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator". In: *IEEE Journal of Solid-State Circuits* 53.8 (2018), pp. 2399–2414.

[129] A. Singh et al. "Improved power side channel attack resistance of a 128-bit AES engine with random fast voltage dithering". In: *ESSCIRC 2017 - 43rd IEEE European Solid State Circuits Conference*. 2017, pp. 51–54.

[130] K. Chae and S. Mukhopadhyay. "All-Digital Adaptive Clocking to Tolerate Transient Supply Noise in a Low-Voltage Operation". In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 59.12 (2012), pp. 893–897.

[131] M. Kar et al. "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*. 2016, pp. 453–456.

[132] M. K. Yadav, M. R. Casu, and M. Zamboni. "DVFS Based on Voltage Dithering and Clock Scheduling for GALS Systems". In: *2012 IEEE 18th International Symposium on Asynchronous Circuits and Systems*. 2012, pp. 118–125.

[133] B. H. Calhoun and A. P. Chandrakasan. “Ultra-dynamic Voltage scaling (UDVS) using sub-threshold operation and local Voltage dithering”. In: *IEEE Journal of Solid-State Circuits* 41.1 (2006), pp. 238–245.

[134] Tobias Schneider and Amir Moradi. *Leakage Assessment Methodology - a clear roadmap for side-channel evaluations*. Cryptology ePrint Archive, Report 2015/207. `https://eprint.iacr.org/2015/207`. 2015.

[135] Monodeep Kar et al. “Blindsight: Blinding EM Side-Channel Leakage using Built-In Fully Integrated Inductive Voltage Regulator”. In: *CoRR* abs/1802.09096 (2018). arXiv: `1802.09096`.

[136] M. Alioto et al. “Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits”. In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 57.2 (2010), pp. 355–367.

[137] David Oswald and Christof Paar. “Improving Side-Channel Analysis with Optimal Linear Transforms”. In: *Smart Card Research and Advanced Applications*. Ed. by Stefan Mangard. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 219–233. ISBN: 978-3-642-37288-9.

[138] A. Singh et al. “Mitigating Power Supply Glitch based Fault Attacks with Fast All-Digital Clock Modulation Circuit”. In: *2019 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2019, pp. 19–24.

[139] M. Khairallah et al. “DFARPA: Differential fault attack resistant physical design automation”. In: *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2018, pp. 1171–1174.

[140] W. Yu and S. Kse. “A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks”. In: *IEEE Transactions on Circuits and Systems I: Regular Papers* 63.8 (2016), pp. 1152–1163.

[141] W. Yang et al. “An enhanced-security buck DC-DC converter with true-random-number-based pseudo hysteresis controller for internet-of-everything (IoE) Devices”. In: *2018 IEEE International Solid - State Circuits Conference - (ISSCC)*. 2018, pp. 126–128.

[142] A. Singh et al. “25.3 A 128b AES Engine with Higher Resistance to Power and Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low-Dropout Regulator”. In: *2019 IEEE International Solid- State Circuits Conference - (ISSCC)*. 2019, pp. 404–406.

[143] A. Singh et al. “Enhanced Power & Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO”. In: *under review with IEEE Journal of Solid-State Circuits* (2019).

[144] N. Chawla et al. “Extracting side-channel leakage from round unrolled implementations of lightweight ciphers”. In: *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2019.

[145] R. Gilmore, N. Hanley, and M. O’Neill. “Neural network based attack on a masked implementation of AES”. In: *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2015, pp. 106–111.

[146] Loc Masure, Ccile Dumas, and Emmanuel Prouff. *A Comprehensive Study of Deep Learning for Side-Channel Analysis*. Cryptology ePrint Archive, Report 2019/439. `https://eprint.iacr.org/2019/439`. 2019.

[147] Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. “Convolutional Neural Networks with Data Augmentation Against Jitter-Based Countermeasures”. In: *Cryptographic Hardware and Embedded Systems – CHES 2017*. Ed. by Wieland Fischer and Naofumi Homma. Cham: Springer International Publishing, 2017, pp. 45–68. ISBN: 978-3-319-66787-4.

[148] Julien Doget et al. “Univariate side channel attacks and leakage modeling”. In: *Journal of Cryptographic Engineering* 1.2 (2011), p. 123.

[149] G. Dabosville, J. Doget, and E. Prouff. “A New Second-Order Side Channel Attack Based on Linear Regression”. In: *IEEE Transactions on Computers* 62.8 (2013), pp. 1629–1640.

[150] Santos Merino Del Pozo and Franois-Xavier Standaert. *Blind Source Separation from Single Measurements using Singular Spectrum Analysis*. Cryptology ePrint Archive, Report 2016/314. `https://eprint.iacr.org/2016/314`. 2016.

[151] Nikhil Chawla et al. *Application Inference using Machine Learning based Side Channel Analysis*. 2019. arXiv: `1907.04428 [cs.CR]`.

[152] Santos Merino Del Pozo and Franois-Xavier Standaert. *Blind Source Separation from Single Measurements using Singular Spectrum Analysis*. Cryptology ePrint Archive, Report 2016/314. `https://eprint.iacr.org/2016/314`. 2016.

[153] François-Xavier Standaert, Tal G. Malkin, and Moti Yung. “A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks”. In: *Advances in Cryptology - EUROCRYPT 2009*. Ed. by Antoine Joux. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 443–461. ISBN: 978-3-642-01001-9.

[154] Alia Levina, Daria Sleptsova, and Oleg Zaitsev. “Side-channel Attacks and Machine Learning Approach”. In: *Proceedings of the 18th Conference of Open Innovations Association FRUCT*. FRUCT ’18. Saint-Petersburg, Russia: FRUCT Oy, 2016, pp. 181–186.