Design and Analysis of Countermeasures for Securing IoT Edge Devices Against Power Analysis Attacks

A
thesis submitted
for the award of degree of

DOCTOR OF PHILOSOPHY

Submitted by

Thockchom Birjit Singha

Under the supervision of

Prof. Roy Paily Palathinkal and Prof. Shaik Rafi Ahamed

Department of Electronics and Electrical Engineering
Indian Institute of Technology, Guwahati
Assam, India - 781039
September, 2024

Dedicated to
"My Beloved Grannies" ,
who I lost during the course of my PhD journey

DECLARATION

*This is to certify that the thesis entitled "**Design and Analysis of Countermeasures for Securing IoT Edge Devices Against Power Analysis Attacks**", submitted by me to the Indian Institute of Technology, Guwahati for the award of the degree of **Doctor of Philosophy** is a bonafide work carried out by me under the esteemed supervision of **Prof. Roy Paily Palathinkal and Prof. Shaik Rafi Ahamed**. The contents of this thesis, in full or in parts, have not been submitted to any other institute or university for the award of any degree or diploma.*

Signed: _____

Thockchom Birjit Singha
Department of Electronics and Electrical Engineering
Indian Institute of Technology, Guwahati
Assam, India - 781039

Date: _____

CERTIFICATE

*This is to certify that the thesis entitled "**Design and Analysis of Countermeasures for Securing IoT Edge Devices Against Power Analysis Attacks**", submitted by **Thockchom Birjit Singha (166102102)**, a Research Scholar in the Department of Electronics and Electrical Engineering, Indian Institute of Technology, Guwahati, for the award of the degree of **Doctor of Philosophy**, is an original research work carried out by him under our supervision and guidance. The thesis has fulfilled all the requirements as per the regulations of the institute and, in my opinion, has reached the standard needed for submission. The contents of this thesis, in full or in parts, have not been submitted to any other institute or university for the award of any degree or diploma.*

Signed: _____

Prof. Roy Paily Palathinkal
Department of Electronics and Electrical Engineering
Indian Institute of Technology, Guwahati
Assam, India - 781039

Date: _____

Signed: _____

Prof. Shaik Rafi Ahamed
Department of Electronics and Electrical Engineering
Indian Institute of Technology, Guwahati
Assam, India - 781039

Date: _____

Acknowledgement

'Guide', 'Mentor', 'Supervisor', are words I had heard about quite often before venturing into PhD. However, had it not been for my supervisor, Prof. Roy Paily Palathinkal, and my co-supervisor, Prof. Shaik Rafi Ahamed, I wouldn't have realized what these words actually mean. The amount of cooperation my supervisor has extended to me since the day I set my foot on this beautiful IITG campus, is beyond my words. I still remember the days, when I regularly stalked his webpage dreaming to be working under him, and as I pen down this acknowledgement, I can claim my dream to be fulfilled. The most striking feature during my time with him is his decision-making which has proven right every single time. Although he always left the final call on me, I knew the thoughts lurking behind his sharp mind. Having studied under strict teachers from Kerala right from my schooling, I was aware of the challenge his strictness would pose to me. Also, he threw me in deep waters trying to ensure I push my boundary of abilities beyond my strength. At the end of the day, the faith I have garnered from him (apart from the technical knowledge and growth, of course) is my most valuable possession I'll bow out of my PhD with.

As for my co-supervisor, our relationship started the day he shot close to 20 questions during my PhD interview. I consider myself very lucky to have been blessed with his supervision. Being a faculty of VLSI architecture, his suggestions regarding my work were very much essential. I cannot forget his one-liner during my visits to his chamber, "You are on the right track", which used to be the ending note to our meetings. The confidence he showed upon me was something which made me pull up my socks, and run this race of so-called PhD. His intricate paper corrections, coloring (red) my manuscripts, has always been a pleasure to my eyes. Most importantly, my research problems have been severely backed by him, even while I had a momentary thought to quit them.

I extend my heartiest thanks to my Doctoral Committee (DC) members, Prof. Harshal B. Nemade, Dr. Sonali Chouhan and Dr. John Jose. Prof. Nemade's understanding of 'hardware' is something everyone praises about, however having a first-hand experience has been a totally different taste. His suggestions have been worth considering which has shaped my thesis in the manner I am submitting. I believe having Dr. Sonali in my DC panel has lent a very significant perspective to my thesis. Her judgement of my work as a 'communication expert' made me thoughtful about how my work can be perceived in a different manner. Finally, the last man standing in my DC, Dr. John, has had a huge role in my PhD work. His inquiries and concerns regarding my work have always challenged me to dig deeper. Apart from my thesis work, he has always been a super-help in my attendance for VLSI Design conferences. And, yes, he writes great recos.

I would also like to take an opportunity to thank Dr. Gaurav Trivedi, who permitted me to use the Synopsys tools housed at his server. During the time, when the IIT fraternity was down without tools' licenses, I could carry on with my work owing to his timely help. I also extend my heartfelt thanks to Dr. Sanjib Das, who has helped me in resolving departmental server-related problems pertaining to MATLAB or other tools.

On the workfront, Mysura Reddy was the first person I clubbed with, Timothy Simon Thomas joined the brigade and we cracked the AES together. God sent Basa Sanjana to rescue me, whose calm and focused energy has elevated our work to a level I wouldn't have been able to, alone. We have been and are, currently, a part of many works, and it's a great feeling to be sharing knowledge with her. I have also been blessed with a work-mate, Titu

Mary Ignatius, who has been the most honest critic of my work. Her inquisitiveness and maturity to look at things from a different level, have helped me immensely. I also had a brief stint with Anupam Kumari, who continues to shoulder responsibilities pertaining to our research group. Surya Srikar is another team member whose deep thinking and sharp mind, has benefited me a lot. Learnt from Dhruv Kumar, too. It's been an honored privilege and absolute pleasure to work with these people.

A glance towards my lab, and I see Josephine Ma'am with her motherly personality. She has been very supportive and all ears to my issues right throughout my PhD. I wouldn't want to miss out on thanking Dr. Vimal Kumar Singh Yadav who strategized in inducting me here to IITG. Having shared a lot of time with him since our M. Tech. days, he has always acted as an elder brother to me. A huge credit of my work to Dr. Satyajit Bora, another classmate from M. Tech. times, who happened to be working under the same supervisor, as Vimal and me. His assistance regarding tools and in personal capacity has been really instrumental in me coming this far. Also, remembering my lab seniors who I happened to meet upon joining PhD here- Dr. Pavan Kumar Manchi, Dr. Saroj Mondal, Dr. Vinaya M M, Dr. Brajesh Rawat, and Dr. Rajan Singh. Another lab-mate whose support I can't overlook is Sampriti Ghosh, who has always been there for me, to share our good and bad, apart from helping me with my technical work. Also, always standing by me, has been Rahul Sharma, who has always been open to discussions leading to positive conclusions and happiness throughout.

A heap of lab mates to thank for keeping the lab, a happy space, Dr. Pralay Chakrabarty, Dr. Raveesh S, Mridul Goswami, Aditi Paul, Guljar Ansari, Praveen Saraswat, Uday Maurya, Radharani Yumlembam, Firoz Shah, Tsiiveikho Saphou, Ashagrie M Kemie, Shiva Prasad, Shashank Srivastava and Surabhi Mishra.

On to my friends' league, a lot of names.. Pingpasara Mantaw, Kalyani Namchoom, Woipeng Manpoong, Mridul Baruah, Mamtha Mathew, Priya Prasun, Pranjal Prasun, Shikhar Saraswat, Th. Debika, Dr. Arunima Dutta, Dr. Jinti Hazarika, Dr. Arijit Roy, Dr. Monica N, Sophia L, Menan Lc, Dr. Lenin L, Susma Th, Ksh. Priyalakshmi, Thuleshwar Lahan, Nishant Anurag, Aditya Pawar, Sanjib Mog, Dr. Samarjeet Das, Dr. Prateek Rathore, Y Robinson, S Aruna, Th. Nicola, Himanshu Singh, Shiv Jaishi, Debashis Paul, Anik Batabyal, James M, Omesh Y, Dr. Alex Paul, Aikendrajit N, Athoibi S, Guluk A Dutta. Also, can't thank enough, my NIT Silchar colleagues who literally pushed me to do my PhD from an IIT, Dr. Munmun Khanra, Dr. Sudarsan Sahoo, Dr. Ranjith Nair, and Dr. Abhishek Midya. A special mention to my friends, Atanu Purkayastha and Dr. Hirkah Jyoti Das, for being with me in my worst times. Dr. Manoranjan Minz and Dr. (to be) Sibasis Sahoo are the two most patient people who I nagged during my PhD journey, and thank you for bearing me. Also, earned a very dear friend in the form of Himadri Brahma, towards the fag end of my PhD. Undoubtedly, this journey wouldn't have been complete for me, had it not been for the blessings of all my teachers from whom I have learnt lessons and life.

Finally, my family has been rock solid behind me, throughout this journey. My sister is currently admitted into PhD at NIT Silchar, walking in my footsteps. My mother has been the most patient cheerleader, and my father, the greatest motivator and challenger. Today, on this note, I wish to share his formula for success.

$$\textbf{Success} = \textbf{Luck} \times \textbf{Labour}^2$$

Guwahati
September, 2024

Thockchom Birjit Singha

Abstract

IoT edge devices are plagued by power analysis attacks despite the usage of Advanced Encryption Standard (AES) as a part of securing information exchange. However, owing to the resource constraint environment offered by the IoT environment, an AES design consuming low resources with an embedded countermeasure providing high security ensuring minimal area and power overheads, is the need of the hour. This thesis presents four cumulative approaches in designing a countermeasure for AES to thwart the attacks. The first step is the wise choice of Masoleh S-box against other available S-boxes, providing minimal switching and enhanced nonlinearity. The second stride is by designing a novel Cipher Feed Back-64 mode inspired by the standard modes of AES operation. The third scheme is by splitting the SubBytes round operation into multiple clocks to reduce side-channel leakage. Finally, a novel expansion-compression Random Number Generator (RNG) assisted with buffer-based delay element is proposed to corrupt the meaningful samples of AES, acquired by the attacker. Analysis of hardware security metrics, like Measurements To Disclose (MTD), Signal-to-Noise Ratio (SNR), Mutual Information (MI) and Test Vector Leakage Assessment(TVLA) render this proposed four-dimensional approach to be highly resilient against the attacks, with minimal area and power overheads. The testing of the designs are performed for Application Specific Integrated Circuit (ASIC) using Synopsys and Cadence tools with UMC 65 nm technology node, and on Field Programmable Gate Array (FPGA) using Side-channel Attack Standard Evaluation BOard (SASEBO). Upon amalgamation of all the four works into one, the results showed negative area and power overheads of -2.91% and -5.61 %, respectively, when referenced with an AES design with LUT-based S-box, apart from being resilient to CPA attack with 1 million plaintexts. A compromise in throughput is incurred owing to the usage of excessive clocks, however satisfying the moderate-speed IoT applications.

CONTENTS

Chapter 1: Introduction 1

1.1 Is information secure in IoT edge devices? . . . 3
1.2 Does AES provide enough security? . . . 4
1.3 How do attackers steal information? . . . 6
1.4 What defines a device's security level? . . . 11
1.5 Problem formulation and thesis organization . . . 14

Chapter 2: Literature survey 17

2.1 AES design strategies befitting IoT hardware resources constraints . . . 18
2.2 Countermeasure attempts to secure AES designs . . . 27
2.2.1 Hiding-based countermeasures . . . 28
2.2.2 Masking-based countermeasures . . . 41

Chapter 3: S-box hardware analysis to improve AES' intrinsic security 49

3.1 S-boxes under investigation . . . 50
3.1.1 Canright S-box . . . 51
3.1.2 CMT S-box . . . 51
3.1.3 Maximov S-box . . . 51
3.1.4 Masoleh S-box . . . 52
3.2 Evaluating the investigated S-boxes . . . 52
3.2.1 Hardware resources analysis of the S-boxes . . . 52
3.2.2 Hardware complexity/Linearity analysis of the S-boxes . . . 53
3.2.3 Hardware security analysis of the S-boxes . . . 53
3.3 Chapter summary . . . 57

Chapter 4: Improvement of AES' resilience with novel CFB mode 59

4.1 Proposed rolling architectures for AES modes . . . 60
4.1.1 Hardware efficient architectures for various modes . . . 61
4.1.2 Novel CFB-64 mode for improved security . . . 62
4.2 Establishment of the proposed attack model . . . 63

4.3 Novelty of the proposed architectures . . . 64
4.4 Hardware security metrics evaluation . . . 66
4.4.1 Security metrics' trends depicted by the investigated modes . . . 66
4.4.2 Security metrics evaluation of the proposed CFB-64 mode . . . 66
4.5 Chapter summary . . . 68

Chapter 5: Splitting the SubBytes operation for a countermeasure effect. 71
5.1 Role of SubBytes' round operation in countermeasure design process . . . 72
5.2 SubBytes implementation across multiple clocks . . . 73
5.3 Analyses of the various SubBytes implementation . . . 74
5.3.1 Trace pattern comparison . . . 74
5.3.2 Hardware resources analysis . . . 74
5.3.3 Security analysis of the investigated designs . . . 76
5.4 Proposed clocking strategy . . . 76
5.5 Novelty of the proposed design . . . 77
5.6 Security analysis of the proposed design . . . 78
5.7 Chapter summary . . . 80

Chapter 6: Compression and Expansion-based countermeasure design assisted with buffer delays 81
6.1 Countermeasure design strategy . . . 82
6.1.1 Disturbing the AES' power trace amplitude . . . 82
6.1.2 Attempt to disorder the timing of SubBytes operations . . . 84
6.2 Trace pattern analysis . . . 85
6.3 Novelty of the proposed design . . . 87
6.4 Security metrics analysis . . . 87
6.5 Comparison with state-of-the-art designs . . . 89
6.6 Chapter summary . . . 91

Chapter 7: Conclusion and future directions 93

LIST OF TABLES

1.1 Quantiles, z_α distribution for some values of α 11

2.1 S-Box (AES) Hardware Resources Utilization 23
2.2 Hardware resources and security metrics of various countermeasures 45

3.1 Resources comparison of various S-boxes and their AES implementation on UMC 65 nm technology node 52
3.2 Hardware resources comparison of various S-boxes and their AES implementation on UMC 65 nm technology node 53
3.3 Comparison of Maximov and Masoleh S-box-employed-AES designs w.r.t. earlier unprotected AES designs 57

4.1 Hardware resources comparison of various AES modes on ASIC 63
4.2 Hardware resources comparison of various AES modes on FPGA 63
4.3 Proposed countermeasure vs. state-of-the-art designs 68

5.1 Hardware resources comparison of various clocking strategies on ASIC and FPGA 74
5.2 Proposed countermeasure vs. state-of-the-art designs 78

6.1 Comparison of the proposed countermeasure w.r.t. state-of-the-art designs. . 89
6.2 Comparison of the proposed countermeasure w.r.t. state-of-the-art designs. . 90

LIST OF FIGURES

1.1 An IoT ecosystem with a node under SCA. 2
1.2 Side-channel monitoring. 3
1.3 AES design flow. 4
1.4 Key scheduler. 5
1.5 HD model attacking the AES 10^{th} round. 7
1.6 CPA attack model. 8
1.7 ASIC methodology. 9
1.8 FPGA methodology. 10
1.9 Quantiles z_α of the normal distribution $N(0,1)$ for some α values. 12

2.1 Classification of S-box design principles 21
2.2 Year-wise depiction of countermeasures 27
2.3 Random power-based hiding countermeasures 35
2.4 Equal power-based hiding countermeasures 40
2.5 Masking-based countermeasures 44

3.1 Share of linear and nonlinear gates for the S-boxes 54
3.2 AES power trace comparison for different S-boxes 54
3.3 Attack results of sample byte 1 for Maximov S-box-based AES design 55
3.4 Byte wise analysis of hardware security metrics for AES with different S-boxes 56

4.1 Proposed hardware-suitable rolling architectures for AES modes ($\oplus$ represents XOR operator) 61
4.2 Proposed CFB-64 AES mode 62
4.3 Proposed attack models for assessing the AES modes 63
4.4 Hardware security metrics comparison for all the modes on SASEBO and ASIC 65
4.5 ASIC-based security metrics for the proposed CFB-64 mode of operation . . 67
4.6 SASEBO–based security metrics for the proposed CFB-64 mode of operation 67
4.7 TVLA plots for the proposed CFB-64 mode of operation 67
4.8 Security improvements of the proposed CFB-64 mode 68

5.1 Illustration of SubBytes implementation across multiple clock cycles (a) 1-clock, (b) 2-clock, (c) 4-clock, (d) 8-clock, (e) 16-clock implementation . . . 73
5.2 AES trace comparison for SubBytes implementation across different clock cycles 75
5.3 Security comparison of the investigated designs 76
5.4 Proposed clocking strategy utilizing posedge and negedge in an 82-clock design 77
5.5 ASIC-based security metrics for the proposed pos-neg clocking strategy . . . 79
5.6 SASEBO-based security metrics for the proposed pos-neg clocking strategy . 79
5.7 TVLA plots for the proposed pos-neg clocking strategy 79

6.1 Proposed countermeasure based on compression and expansion 82
6.2 Internal structure of 8:16 CEB and 16:8 CCB 83
6.3 Buffer block to delay the S-box operations 84
6.4 Illustration of the effect of buffer-based delays 85
6.5 Layout of AES after incorporation of the countermeasures 86
6.6 ASIC traces of the protected AES design on Synopsys Custom WaveView . . 86
6.7 Trace pattern of AES after incorporation of the countermeasures 86
6.8 ASIC-based security metrics for the proposed countermeasure 88
6.9 SASEBO-based security metrics for the proposed countermeasure 88
6.10 TVLA plots for the proposed countermeasure 88

LIST OF ACRONYMS

AES	Advanced Encryption Standard
NIST	National Institute of Standards and Technology
IoT	Internet of Thing
VLSI	Very Large Scale Integration
PAA	Power Analysis Attack
SCA	Side Channel Attack
DPA	Differential Power Analysis
CPA	Correlation Power Analysis
PSCA	Power Side Channel Attack
PRNG	Pseudo Random Number Generator
LFSR	Linear Feedback Shift Register
EM	Electro Magnetic
GF	Galois Field
HD	Hamming Distance
HW	Hamming Weight
ASIC	Application Specific Integrated Circuit
FPGA	Field Programmable Gate Array
DC	Design Compiler
GSa/s	Giga Samples per second
MTD	Measurements To Disclose

SNR	Signal to Noise Ratio
MI	Mutual Information
TVLA	Test Vector Leakage Assessment
S-box	Substitution Box
LUT	Look Up Table
GE	Gate Equivalent
CFA	Composite Field Arithmetic
CMT	Circuit Minimization Team
ECB	Electronic Code Book
CBC	Cipher Block Chaining
CFB	Cipher Feed Back
OFB	Output Feed Back
CTR	Counter
IV	Initialization Vector
SASEBO	Side-channel Attack Standard Evaluation BOard
CEB	Comparator and Expansion Block
CCB	Comparator and Compression Block
IC	Integrated Circuit
UMC	United Microelectronics Corporation

CHAPTER

1

INTRODUCTION

Contents

1.1 Is information secure in IoT edge devices? 3
1.2 Does AES provide enough security? 4
1.3 How do attackers steal information? 6
1.4 What defines a device's security level? 11
1.5 Problem formulation and thesis organization 14

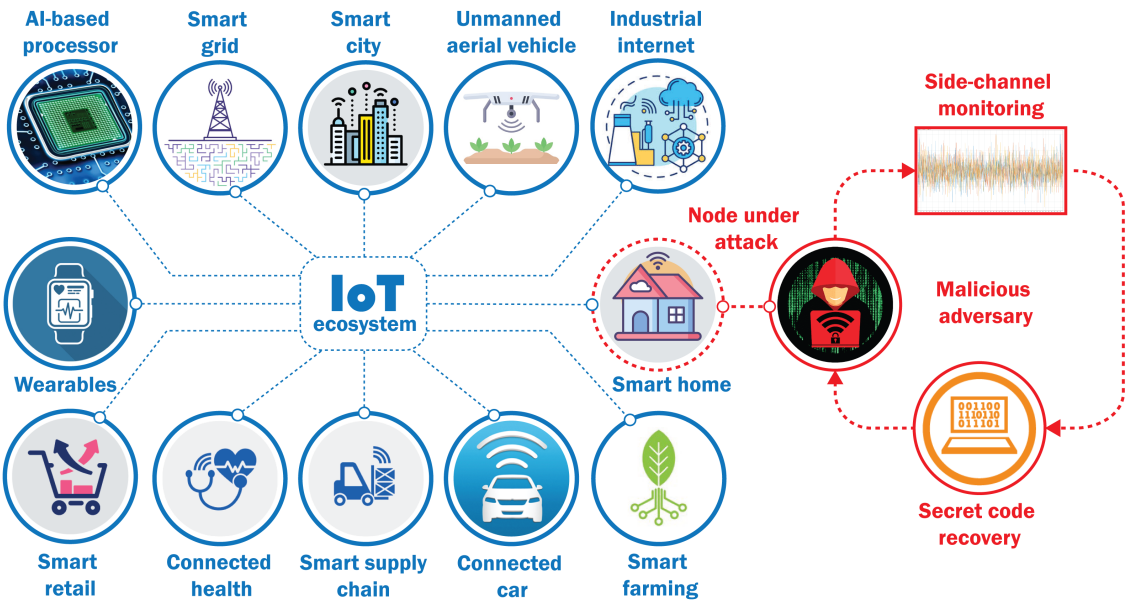


Figure 1.1: An IoT ecosystem with a node under SCA.

Today, the whole world has shrunk into a close knit group owing to the well-laid communication technologies. The chunk of information and distance, too, vary from kilobytes of data for bluetooth applications, to terabytes of data over Internet. Despite these diversities, the significance of information and its security involved, across such a wide spectrum, is all the same. Although the public academic research in cryptography came to the forefront towards the end of the 20^{th} century, the seeds were sown during World War II where a mechanical encryption device like rotor performed general substitution of numbers and letters, to hide information from the enemy. State-of-the-art computer cryptography is employed outside the secured boundaries of military agencies, covering all information transfer applications. A very noteworthy point is that the beneficiaries of cryptography range from a layperson to the nation's highest administrator. Day-to-day technological applications include end-to-end encryption in messaging, protecting stored files in a computer, disk encryption of operating systems, device locking, private networks, web browsing, etc. Few practical examples advocating the need for information security are designing a new product or framing a market strategy by a business company, a campaign plan by a political party, discussion on taxes by the government, citizens living in a country with no rights to privacy, etc.

Amongst the diverse cryptographic applications, the one which has drawn the most significant attention of the researchers worldwide is 'Internet'. Spreading its tentacles to every nook and corner of the globe, it has become the most extensively used mode of communication today. One of its majorly used forms that has been grabbing everyone's eyeballs is the 'Internet of Thing (IoT)'. It refers to the numerous physical devices existing around the world that are associated with Internet, targeting data exchange and assemblage. The most remarkable feature of an IoT system is that the transfer of information over a network does not necessitate a human-to-human or a human-to-computer interaction. An IoT device communicates with other related devices and process the information received from each other. The prime share of their tasks is carried out without human intervention although they are authorized to provide instructions, access data or set them up. The surge in IoT users is tipped to increase manifold in the upcoming years, from the current 12 billion mark. Similar to a coin having two sides, IoT-based communication suffers from the jeopardy of information breach despite providing extended connectivity.

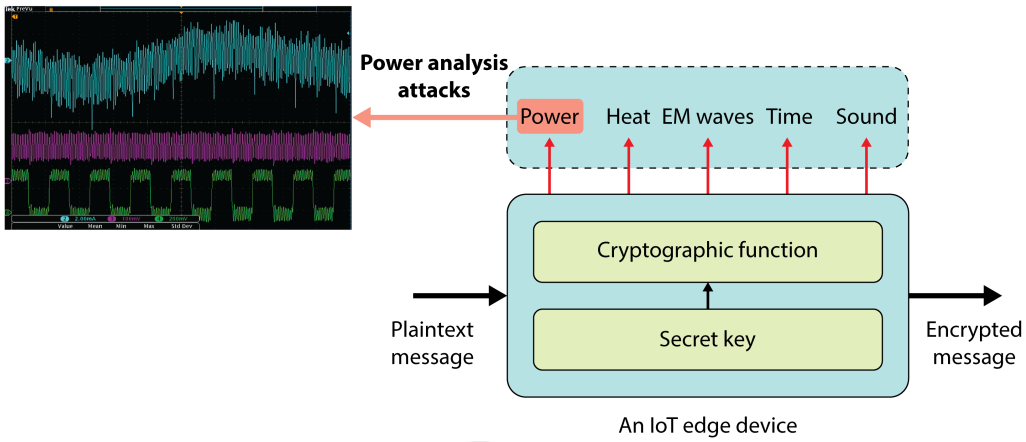


Figure 1.2: Side-channel monitoring.

1.1 Is information secure in IoT edge devices?

An IoT architecture is characterized by three layers, namely, application, network and perception. Adversaries adopt different strategies to attack each layer. Structured Query Language (SQL) injection [1] and phishing attack [2] are performed on the application layer, state-based [3] and AI-based attacks [4] are employed at the network layer, whereas RF jamming [5] and side-channel attacks [6] threaten the perception layer. The IoT architecture employs numerous edge devices to relay information across networks. These devices are under severe threat from adversaries owing to their easy accessibility in the sensor networks. In contrast to earlier techniques, where devices were broken upon to thieve information from them, noninvasive methods have flourished in recent times. SCA is one such form which targets IoT devices by monitoring some physical properties emancipated by them while performing cryptographic operations. Such a phenomenon is called side-channel monitoring, where the physical properties are observed and tracked to retrieve secret codes implanted in the devices. Figure 1.1 portrays an IoT ecosystem with diverse applications, where a node is under SCA.

Based on side-channel parameters, such as power, timing, electromagnetic (EM) radiations, heat, and sound, the cryptographic operations can be decoded. Power and EM radiations tend to be the most vulnerable parameters among these and are termed Power Analysis Attacks (PAAs) [7] and EM analysis attacks [8], respectively. Side-channel analysis of malicious foreign logic like hardware Trojans, are aimed at detecting changes to the intrinsic behavior of a manufactured integrated circuit (IC) [9].

Side-channel monitoring involves observance of power patterns, Electro Magnetic (EM) waves, timing information, heat, sound, etc., termed as ‘side channel parameters’. Figure 2 illustrates the principle of side-channel monitoring in an IoT edge device. SCA of IoT edge devices targets recovery of secret cipher key information embedded in the cryptographic hardware. Ciphers employing different secret keys at the sender and receiver terminals are called assymetric ciphers, whereas the ones employing the same secret key are called symmetric ciphers. Assymetric ciphers, such as, Elliptic Curve Cryptography (ECC) and Rivest Shamir Adleman (RSA) are engaged in modern day technologies like digital signatures, financial transactions over Internet, etc. On the other hand, symmetric ciphers, such as, International Data Encryption Algorithm (IDEA), Rivest Cipher 4 (RC4), Advanced Encryption Standard (AES), etc. find use in electronic voting systems, Local Area Network (LAN), processor security, etc. Some examples of practical attacks are the Apple CoreCrypto being

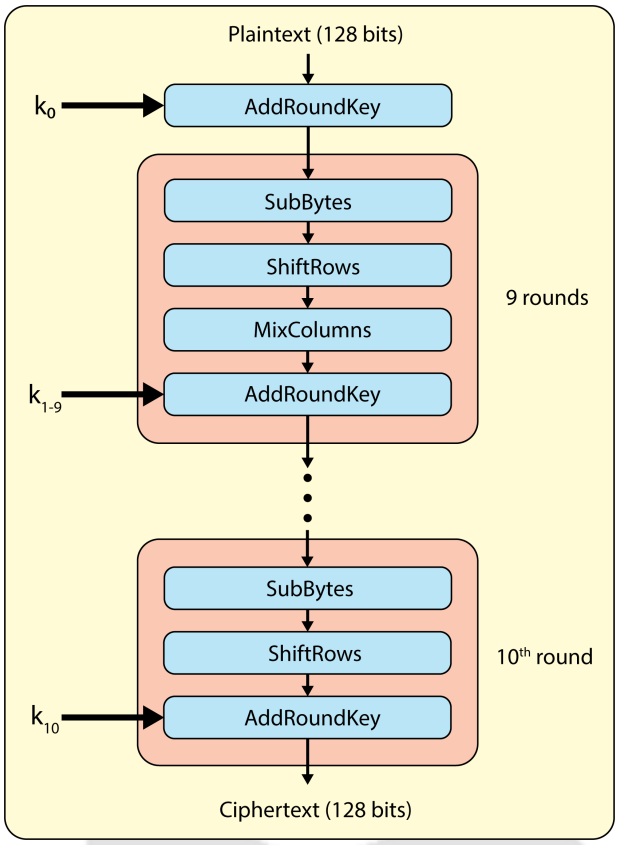


Figure 1.3: AES design flow.

successfully hacked, the Philips Hue lightbulbs being turned on and off, and the Platypus attack on Intel server, desktop and laptop CPUs to gain unprivileged access to infer data and extract cryptographic keys, by attackers.

Assessing the need for security of IoT edge devices and keeping in view their hardware resources constraints invovled, AES emerged to be the most favorable cipher amongst all other ciphers. Its lightweight nature coupled with the provided nonlinearity and diffusion, makes it the most suitable cryptographic algorithm for securing information exchange involved in such devices. National Institute of Standards and Technology (NIST) proposed AES as the replacement of Data Encryption Standard (DES) in 2001, owing to the latter's brittle resistance to 'attacks'. Today, AES is an automatic choice in multiple IoT standards, such as IEEE 802.11i [10], IEEE 802.15.4 [11], ZigBee [12], and IoT proposals, such as SiGFox, ZWave and LoraWAN.

1.2 Does AES provide enough security?

AES is a symmetric block cipher which works on a 128-bit data at the sender's and receiver's terminal [13]. It is a type of Substitution Permutation Network (SPN) implementable in 10, 12 and 14 rounds for key lengths of 128-bit, 192-bit and 256-bit, respectively. The scope of this thesis limits to AES-128, implying a 128-bit key length. The PN is facilitated by four round operations which involve AddRoundKey performing the whitening step, SubBytes fulfilling the substitution step, and ShiftRows and MixColumns accomplishing the permutation step. For an AES adopting a 10-round strategy for encryption, a remarkable feature is that the last round is bereft of the MixColumns step. The AES flow mechanism is represented in figure 1.3, with its round operations and key scheduling operations, described as follows.

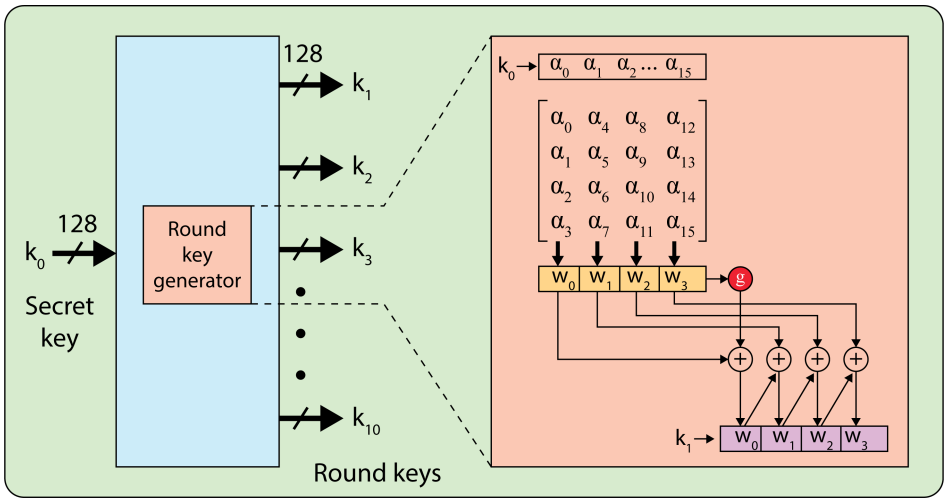


Figure 1.4: Key scheduler.

Round operations.

The round operations are performed on the original plaintext to eventually transform it to an unrelatable ciphertext. The deeper the plaintext gets into the algorithm, or the more the round operations act upon it, the lesser is its correlation between the intermediate round outputs and the plaintext. The 128-bit plaintext is stored in the form of a 4×4 state matrix with each matrix element representing a byte. A four-step strategy is adopted as a part of the round operation: -

1. **AddRoundKey**. This is the first step of an AES algorithm which involves xoring of the plaintext with the secret cipher key.

2. **SubBytes**. An acronym for Substitution of Bytes, the SubBytes step, as the name suggests, substitutes each byte of the plaintext with another pre-decided byte. This operation is performed on the basis of a Substitution Box (S-box) which has pre-computed alternative for every possible value of a byte. The S-box entries have been calculated using Galois Field (GF) mathematics to provide nonlinearity to the SubBytes operation. This step involves 16 S-box operations owing to the 16 bytes in state matrix.

3. **ShiftRows**. The AES round operation is a permutation step which cyclically shifts the rows of the state matrix. Leaving the first row unchanged, the second row is shifted right by one place, the third row is shifted by two, and the fourth row is shifted by three positions.

4. **MixColumns**. This is the second permutation step with operations on the columns of the state matrix. The elements of the column in the matrix is considered as a four-term polynomial over GF(2^8) and multiplied with a fixed polynomial,

$$a(x) = 03x^3 + 01x^2 + 01x + 02 \tag{1.1}$$

. In order to restrict the degree of the resultant polynomial to 3, a multiplication modulus of $(x^4 + 1)$ is used. The MixColumns operation can be represented as:

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} \tag{1.2}$$

Key scheduling operations.

AES transforms a plaintext into a ciphertext using a secret cipher key. However, the algorithm necessitates a round key for each round in the AddRoundKey operation. The round keys are generated from the cipher key using a g-function in a manner as shown in figure 1.4. The g-function involves 1-byte circular left shift SubWord (substitution of a word using S-boxes) and xoring with some constants, Rcon. The round keys can be computed prior to the AES getting underway, and stored in memory, or can be determined on-the-fly as and when required in the round operations.

Vulnerability of AES

With various hardware applications requiring the security feature, AES finds itself in use in many of them. Due to the shrinking size of the devices employed today, the first target of the designers is to reduce the size of AES to fit into the hardware modules. This design target involves focussing on reducing the gate count of the whole AES design by adopting various strategies like using various types of Galois Field (GF): $GF(((2^2)^2)^2)$ and $GF((2^4)^2)$, or technology like tri-gate high-k metal-gate CMOS, etc. The power consumption of AES is usually taken care by optimizing SubBytes design using one-hot encoding, lowering glitching activities, using Pass Transistor Logic, etc.

However, the main purpose of AES being securing data, it still remains vulnerable. IoT edge devices employing AES are an easy target of side-channel attackers. Out of the various side-channel parameters, this thesis limits its scope to 'power', hence the attacks are called "power analysis attacks". The reason behind consideration of this attack is that it is the strongest type owing to the direct correlation between the level of power consumption in CMOS devices and the operations that the device is performing. As the attackers intend to study the power information liberated by the cryptographic operations in the device, SubBytes, the most power intensive step of AES is the target. The SubBytes executes 16 S-boxes to substitute 16 bytes of data, resulting in 75% of the total AES power consumption. The attackers take hints from this AES round operation where majority of the power spending is concentrated. The objective of the attacker is to retrieve the secret cipher key employed in the algorithm, obtaining which reverse engineering can be easily performed to obtain the original messages (plaintexts).

1.3 How do attackers steal information?

Power analysis attack was discovered by Kocher et al. [14] in 1999 which employed power as the side-channel parameter to recover the ciphers secret key. Such attacks reveal the secret keys of cryptographic devices by recording a large number of power traces while the devices perform encryption or decryption on different data blocks. The dependency of cryptographic devices on the data processed is exploited by the attack. The recorded power traces are analyzed at fixed time instants as a function of the intermediate data being processed.

The most common way of generating side-channel information is to gather a large number of power traces by repeatedly running the device using AES. A practical example can be transferring some meagre amount of money, to and from the electronic purse. PAAs generally involve two parameters for a statistical analysis, owing to which they are also known as Differential Power Analysis (DPA) attacks. The parameters involved in DPA, generally, are correlation coefficient, distance-of-means, difference-of-means, and maximum likelihood.

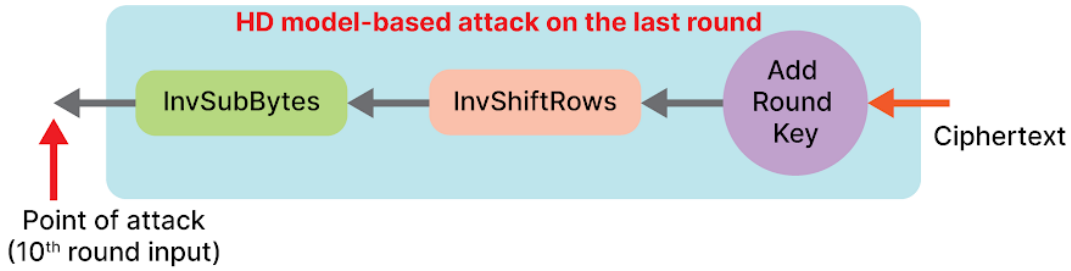


Figure 1.5: HD model attacking the AES 10^{th} round.

DPA based on correlation coefficient requires the least number of power traces to recover the key, which is termed as Correlational Power Analysis (CPA) attack. The forthcoming thesis description narrows its scope to CPA attacks alone.

The AES' power consumption is predominantly the dynamic power consumption of CMOS gates which are data dependent and caused primarily due to switching in the gates. The dynamic power can be considered to be originating from two different components. The first component of dynamic power is the charging power of the load capacitances, represented as in (1.3). $p_{chrg}(t)$ denotes the instantaneous charging power, α represents the activity factor, C_L symbolizes the load capacitance and V_{DD} stands for the supply voltage [15].

$$P_{chrg} = \frac{1}{T}\int_0^T p_{chrg}(t)\,dt \; = \alpha.f.C_L.V_{DD}^2 \tag{1.3}$$

The second component of the dynamic power is due to the short-circuit current caused during the switching of the output. It is represented by (1.4) with $p_{sc}(t)$ denoting the instantaneous short-circuit power, I_{peak}, representing the peak current during the switching event and t_{sc} designating the time for which the short circuit exists.

$$P_{chrg} = \frac{1}{T}\int_0^T p_{sc}(t)\,dt \; = \alpha.f.V_{DD}.I_{peak}.t_{sc} \tag{1.4}$$

The dynamic power thus liberated contains a lot of information about the internal processing of the information and the cryptographic algorithm. It is utilized by the CPA attack to recover the 128-bit key adopting a divide-and-conquer strategy by dividing the key to 16 bytes and cracking them byte-by-byte [15]. The key presents a complexity of 2^{128} possibilities for a brute-force attack which is expected to involve a computer for trillion years. However, a key byte represents only 256 (2^8) possibilities thereby making the key guess a lot easier. The attack model involves collection of AES power traces for multiple plaintexts. For every ciphertext, a series of inverse AES operations in the last round (AddRoundKey, InvShiftRows and InvSubBytes) is performed which involves the 10^{th} round key. The Hamming Distance (HD) transitions during the sequence of operations are recorded and processed, as represented in (1.5):

$$h_{i,j} = HD(v_{i,j}, d_i) = HW(v_{i,j} \oplus d_i) \tag{1.5}$$

where, h denotes the hypothetical power consumption values, d represents the data blocks to be encrypted and v represents the hypothetical intermediate values (corresponding to AES' last round). Power values are assigned to the hypothesized HD transitions, which are compared with the real power values obtained for the generated traces to find the key involved in the encryption process. The HD values are resultant of Hamming Weight (HW) of the outcome obtained by XORing the corresponding v and d values.

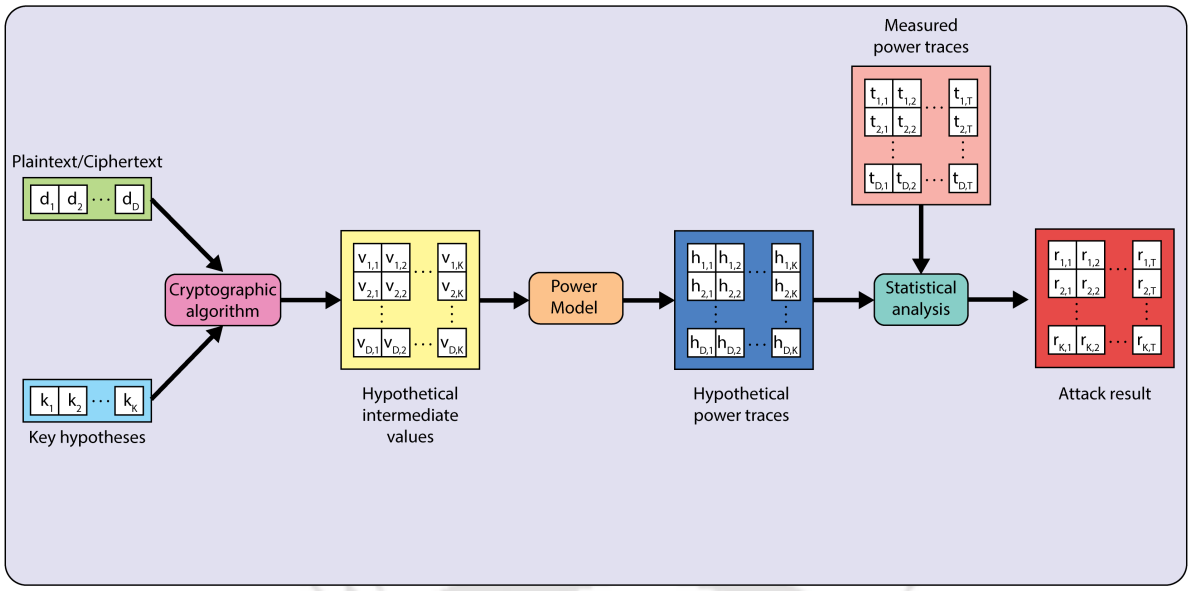


Figure 1.6: CPA attack model.

PAAs employ a 5-step general attack strategy, as illustrated in figure 1.6 [15]:

(1) Choosing an intermediate result of the algorithm.

An intermediate result within the cryptographic algorithm needs to be chosen at the outset, which can be represented as a function $f(d, k)$, with d as the known non-constant data value and k as a small portion of the key. Normally, d is considered to be either the plaintext or the ciphertext.

(2) Measuring the power consumption.

The next step involves measuring the cryptographic device's power consumption while the encryption/decryption of D different data blocks are running. For each run, the attacker seeks the corresponding value of d, involved in the intermediate result (chosen in step 1). During each of these runs, the power traces are recorded, with $t_i^{'} = (t_{i,l}, \ldots, t_{i,T})$ denoting the power trace for a block, d_i, where T refers to the trace length. Traces are recorded for each of the D data blocks and stored as a matrix $D \times T$.

(3) Calculating hypothetical intermediate values.

Following the power traces measurement, a hypothetical intermediate value is calculated for every possible choice of k. Key hypotheses are represented by a vector, $k = (k_1, \ldots, k_K)$, where K denotes the total number of possible choices for k. For all D encryptions and K key hypotheses, the hypothetical intermediate values, $f(d, k)$, are evaluated by an attacker resulting in a matrix V of size $D \times K$, whose elements are represented by:

$$v_{ij} = f(d_i, k_j); i = 1, ..., D; j = 1, ..., K \tag{1.6}$$

k_{ck} denotes the key used in the device and knowing the column of V processed during the D encryptions/decryptions gives us the knowledge of k_{ck}.

(4) Mapping intermediates to power consumption values.

This step features the mapping of the hypothetical intermediate values, V, to a matrix H of hypothetical power consumption values, $h_{i,j}$, using Hamming Distance (HD) and Hamming Weight (HW) power models.

(5) Comparing the hypothetical power consumption values with the power traces.

Finally, the attacker correlates the hypothetical power consumption values of each key hypothesis with the measured power traces at every position by comparing the columns of

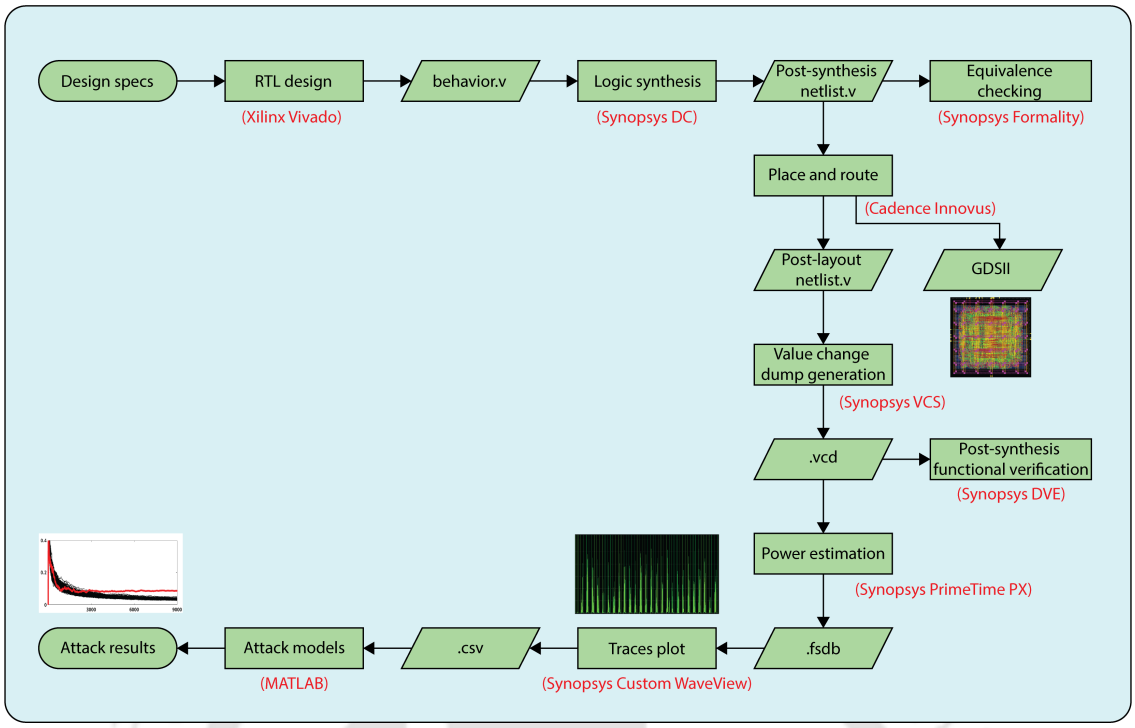


Figure 1.7: ASIC methodology.

the H and T matrices. The resultant is a matrix R of size $K \times T$, whose each element, r_{ij}, is an outcome of the comparison between the elements, h_i and t_j. The values of power consumption in the measured traces contain values depending on the intermediate values, v_{ck}, which is the column, t_{ct} , thereby successfully acquiring the knowledge of the key.

In order to establish the linear relationships between the column data of H and T, 'correlation coefficient' can be used as a parameter for evaluation, resulting in a Correlational Power Analysis (CPA) attack. The correlation coefficient is used to determine a linear relationship between the columns, h_i and t_j, for $i = 1, ..., K$ and $j = 1, ..., T$. A resultant matrix, R, comprising of estimated correlation coefficients, $r_{i,j}$, is estimated based on the D elements of the columns, h_i and t_j. In the following equation, the values $\bar{h_i}$ and $\bar{t_j}$ denote the mean values of the columns, h_i and t_j.

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \bar{h_l}).(t_{d,j} - \bar{t_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \bar{h_i})^2.\sum_{d=1}^{D}(t_{d,j} - \bar{t_j})^2}} \tag{1.7}$$

Attackers employ this attack model to retrieve the secret cipher key from the IoT edge devices employing AES for their information security. This thesis presents ASIC and FPGA implementations of AES designs to mimic the real world scenario. Numerous power traces are generated using both the platforms and the attack is performed on them.

Performing PAA on an ASIC-based AES implementation

Some Electronic Design Automation (EDA) tools are used to design an AES ASIC using UMC 65 nm technology node. The methodology sets about with the finalization of design specfications wich are translated into a Register Transfer Level (RTL) logic using Verilog Hardware Description Language (HDL) on the Xilinx Vivado tool. A behavioral design is the resultant which is synthesized into logic gates defined by the technology node, using Synopsys Design Compiler (DC) . The post-synthesis netlist thus generated is compared for

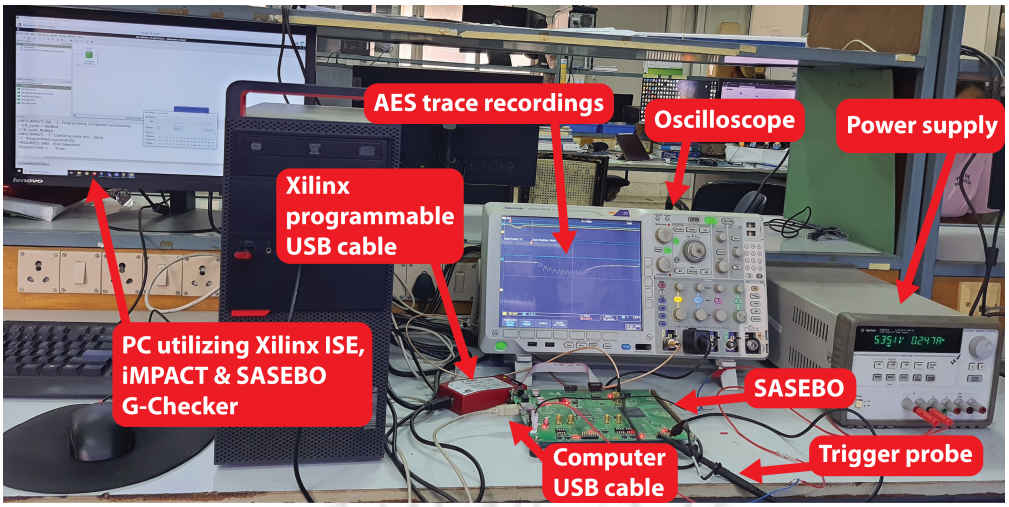


Figure 1.8: FPGA methodology.

its logic equivalence with respect to its RTL design using Synopsys Formality. Once verified, the netlist is used to design the layout of the circuit using Cadence Innovus. The layout process involves further steps like floorplanning, power planning, standard cell placement, clock tree synthesis routing, static timing analysis, design rule check and sign-off . This step results in the GDSII file fit to be sent to the foundry for fabrication, and a post-layout netlist with the effects of parasitics included. The post-layout netlist is passed through Synopsys VCS to generate a Value Change Dump (VCD) file which can store digital logic traces, based on conditions specified in a testbench. The file basically contains a series of time-ordered value changes for the signals. The vcd file is next used by the Synopsys PrimeTime PX to estimate and analyze power dissipation of the netlist containing cell-based designs. A Fast Signal Data Base (FSDB) file is generated which is an event-based format in binary representation, logging each toggle in each signal. The fsdb file is used by Synopsys Custom WaveView to view the generated power traces depicting power values at each time instant. The samples are then recorded from the traces in the form of a Comma Separated Variable (CSV) file at a decided sampling rate (1 GSa/s or 1 sample per nanosecond used for this thesis). The collected trace samples are subjected to PAA models on MATLAB to provide information about the AES design's resilience.

Performing PAA on an FPGA-based AES implementation

The power traces can be generated on hardware platforms like FPGAs, as well. A special FPGA tailormade for side-channel testing is available in the form of Side-channel Attack Standard Evaluation BOard (SASEBO). With other general purpose FPGAs offering a large amount of noise to pick the AES traces from, SASEBO offers a clean trace. It employs a cryptographic FPGA to perform the AES operations alone, and a control FPGA performs the control operations on the board. The cryptographic FPGA utilizes Spartan-3A XC313400DSP while Spartan-3AN XC350AN is employed in the control FPGA. The proper functionality of the board requires it to be powered by an Agilent DC power supply (5V) and a C# program on the PC controls the activities on the board. The bit file of the AES design is generated on Xilinx ISE and an iMPACT software is availed to dump the same on the cryptographic FPGA via the Xilinx programmable USB cable. Post-dumping, the AES design is fed with numerous plaintexts from the SASEBO G-Checker GUI generated out of the C# program. The GUI assists in transferring the plaintexts via the computer USB cable.

The AES operations are invoked by a trigger signal which is captured using a probe, and the generated traces are displayed on a Tektronix MDO4104B-6 Mixed Domain Oscilloscope (MDO) via an SMA-BNC cable. The C# program ensures the traces are stored on the PC in the form of .csv files. A common AES design frequency of 16 MHz is utilized throughout the thesis, which is the maximum permissible frequency of the board. With RFID applications operating at 13.56 MHz, the frequency in use can be considered to be well in the range of IoT applications. Also, in order to model aggressive attack scenarios, a very high sampling frequency of 1 Giga Samples per second (GSa/s) for trace samples collection. Various MATLAB programs on the PC are finally used to evaluate the collected samples pertaining to the AES design, which depict vulnerability or immunity to PAAs.

1.4 What defines a device's security level?

The security level of an IoT edge device under PAA can be judged on the basis of quantitative and qualitative evaluations of some hardware security metrics. The judgement can be passed on the basis of key recovery attacks and information leakage assessments. The former category is an attempt to retrieve the secret cipher key embedded in the device, whereas the latter is a quantitative analysis, if the information siphoned off the device by an attacker is sufficient to label the device as secure or not. Measurements To Disclose (MTD) is a key recovery scheme, whereas Test Vector Leakage Assessment (TVLA) is a leakage assessment ploy. Signal-to-Noise Ratio (SNR) and Mutual Information (MI) are two metrics which fall in both the categories. Each metric is explained as under.

Measurements to disclose (MTD)

In statistics, 'population' comprises of numerous 'samples', where the mean of the parameter in the population is represented by μ. Mean of each sample is termed as average, $\bar{x}$, which is described by a random variable, $\bar{X}$. In accordance with the law of large numbers, an estimation to compute $\bar{X}$ gets better with increasing trace (i.e., points) count. Thus, for the average value to approximate the mean value better, more measurements, n, are needed. A statistical concept called 'confidence interval' helps in understanding the approximation of $\bar{x}$ towards μ. A confidence interval of 0.99 implies an interval containing μ with 0.99 probability.

Hypotheses tests form the bases for confidence intervals. In a hypothesis test, a certain hypothesis is tested whether it is true or not. The first hypothesis is defined as the 'null hypothesis', H_0: $\mu = \mu_0$ whereas the other hypothesis is defined as the 'alternate hypothesis', H_1: $\mu \neq \mu_0$. A confidence interval denotes a range containing all the values that are reasonably close to a certain value for a chosen parameter. All the values μ_0 of the null hypothesis are accepted, which lies in the confidence interval of μ. For a confidence interval, a quantile, z_α, of the standard normal distribution is defined to have the property $p(z \leq z_\alpha) = \alpha$, where, α is called the error probability. A frequently used property is $z_\alpha = -z_{1-\alpha}$. Table 1.1 lists some quantiles.

Table 1.1: Quantiles, z_α distribution for some values of α

α	0.800	0.900	0.990	0.995	0.999
z_α	0.842	1.282	2.326	2.576	3.090

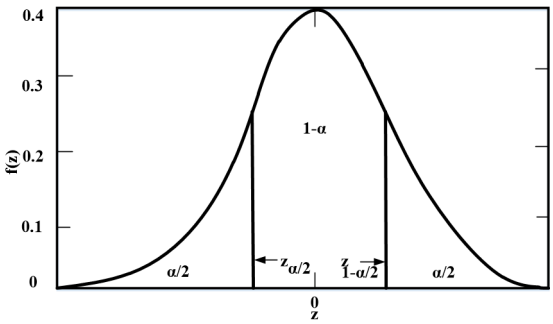


Figure 1.9: Quantiles z_α of the normal distribution $N(0,1)$ for some α values.

Figure 1.9 depicts a standard normal density function showing the quantiles $z_{\alpha/2}$ and $z_{1-\alpha/2}$. From the figure, the probability, $p(z_{\alpha/2} \leq z \leq z_{1-\alpha/2}) = 1-\alpha$. The interval $[z_{\alpha/2}, z_{1-\alpha/2}]$ is the confidence interval for Z. In the confidence interval for μ, the substitution, $Z = (\bar{X} - \mu).\frac{\sqrt{n}}{\sigma}$, needs to be made.

$$i.e., p(\bar{X} - \frac{\sigma}{\sqrt{n}}.z_{1-\alpha/2} \leq \mu \leq \bar{X} + \frac{\sigma}{\sqrt{n}}.z_{1-\alpha/2}) = 1-\alpha \tag{1.8}$$

where, σ is the standard deviation of the normal distribution. For power analysis attacks, the trace count needed to distinguish a certain parameter from zero based on its estimator, is given as:

$$p(\bar{X} < 0) = \alpha,\ given\ \mu = \mu_0\ with\ \mu_0 < 0 \tag{1.9}$$

Hence, the required number of traces 'n' necessary to affirm with confidence $(1-\alpha)$ that the mean of the normal distribution is non-zero, is given by:

$$n = \frac{\sigma^2}{\mu^2}.z^2_{1-\alpha/2} \tag{1.10}$$

Signal-to-noise ratio (SNR)

In each power trace point, the operation-dependent component is referred to as P_{op}, and the data-dependent component of the point as P_{data}. The noise component of the power consumption is denoted as $P_{el.noise}$. The power trace point also comprises of constant components occurring due to transistor switchings which are independent of the performed operations and the processed data, referred to as P_{const}. These components are additive in nature and hence, each point of a power trace is modelled as:

$$P_{total} = P_{op} + P_{data} + P_{el.noise} + P_{const} \tag{1.11}$$

However, for an attacker, only the components, P_{data} and P_{op} are exploitable and are represented together as P_{exp}. Also, the power consumption traces contain switching noise, $P_{sw.noise}$, in addition to electric noise. This noise component is not exploitable in context of a given attack scenario.

$$\therefore P_{op} + P_{data} = P_{exp} + P_{sw.noise} \tag{1.12}$$

$$i.e., P_{total} = P_{exp} + P_{sw.noise} + P_{el.noise} + P_{const} \tag{1.13}$$

The signal and noise component ratio of a measurement is termed as SNR, in the context of PAAs.

$$SNR = \frac{Var(signal)}{Var(noise)} = \frac{Var(P_{exp})}{Var(P_{sw.noise} + P_{el.noise})} \tag{1.14}$$

Higher SNR leads to easy detection of P_{exp} in the noise, thus, implying a leaky cryptographic design. Formally, SNR can also be expressed as a form factor by evaluating the ratio of the maximum correlation coefficient for the correct key, to the highest correlation coefficient corresponding to any other (wrong) key throughout the duration it is processed. Mathematically, it is expressed as [16]:

$$SNR = \frac{\max_{t\in[1...T]} \rho_{t,k_{correct}}}{\max_{t\in[1...T],k\in[1...K]\setminus k_{correct}} \rho_{t,k}} \tag{1.15}$$

where, t: time instant of sampling the power, T: number of samples in a clock cycle, $\rho_{t,k_{correct}}$: correlation coefficients corresponding to correct key, $\rho_{t,k}$: correlation coefficients corresponding to wrong key guesses, k: key search index, also referring to wrong keys, $k_{correct}$: correct key, K: 2^8 for an 8-bit S-box (number of possible key values).

Mutual Information (MI)

It is an information theory approach making use of Shannon's entropy. It quantifies the information leakage for a hardware implementation without using a power model [17]. The quantification of the information leakage by the hardware is brought about using the conditional entropy. A Gaussian distribution for the power samples is assumed for the probability density function.

X and Y are assumed to be random variables on the (discrete) spaces, χ and γ with probability distributions, P_X and P_Y, respectively. The reduction in uncertainty of X that is obtained by having observed Y, is exactly equal to the information that one has obtained on X by having observed Y. Hence, mutual information, $I(X;Y)$, is mathematically represented as:

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = I(Y;X) \tag{1.16}$$

$$I(X;Y) = H(X) - H(X|Y) \tag{1.17}$$

$$I(X;Y) = H(X) - \sum_{x\in X} Pr(x) \sum_{y\in Y} Pr_{chip}(\frac{y}{x}) log_2 Pr_{chip}(\frac{x}{y}) \tag{1.18}$$

where, $H[X]$: entropy of secret variable, X, $Pr(x)$: probability of secret key, $x \in X$, Y: observed leakage, $Pr_{chip}(y/x)$: probability of the leakage, y, given the key, x (it can be derived from $Pr_{chip}(x/y)$ by means of Bayes' theorem). Mutual information satisfies the relation, $0 \leq I(X;Y) \leq H(X)$. The lower bound is attained if and only if X and Y are independent whereas the upper bound is achieved when Y fully determines X. Hence, a larger mutual information signifies closer affiliation between X and Y to a one-to-one relation.

Test Vector Leakage Assessment (TVLA)

Goodwill et al. [18] introduced TVLA as a security metric to signify the amount of information leaked from a cryptographic implementation. It utilizes the widely used statistics tool, the Welch's t-test, to verify whether two given sample sets originate from the same population, by analysing their means. Power traces are recorded based on the key, plaintext and ciphertext used in accordance with the test.

The traces obtained are divided into two disjoint groups, Group 1 and Group 2, upon which two independent Welch tests are to be performed. The Group 1 traces are partitioned

into two subsets, A and B, where, N_A: size of the subset A, N_B: size of the subset B. Further, X_A, X_B, S_A, S_B are computed, where, X_A : average of all the power traces in group A, X_B : average of all the power traces in group B, S_A : sample standard deviation of all the power traces in group A, S_B : sample standard deviation of all the power traces in group B. The t-statistic trace, T , over the same time instants are calculated point-wise for each time instant in the trace for X_A, X_B, S_A, S_B, as:

$$\frac{X_A - X_B}{\sqrt{\frac{{S_A}^2}{N_A} + \frac{{S_B}^2}{N_B}}} \tag{1.19}$$

In the test pertaining to Group-2, the steps are similar to that for Group 1 except that the measurement traces and its corresponding subsets, A and B, will be different. The device is declared to fail if there is any time instant for which the t-test statistic exceeds +c for both group 1 and group 2 or is below -c for both groups. Otherwise, the device is considered to have passed this test. The test vectors to be applied are detailed in [18].

1.5 Problem formulation and thesis organization

Literature portrays widespread design techniques for AES, spanning extensive work on SubBytes and MixColumns round operations, predominantly targeting high throughput to conform to today's high-speed communication. Substitution box (S-box), forms a major share of its research as it forms the core of the algorithm, providing non-linearity and confusion. Another reason for the attention is the fact that it draws 75% of the total AES power consumption. Apart from the concern towards AES hardware resources, another pressing need is its susceptibility towards PAAs. With researchers in the quest of adding countermeasures in order to thwart such malicious attacks, they impose a lot of area and power overheads to the AES design, thereby disqualifying them to meet the stringent area and power requirements, posed by IoT devices.

This thesis intends to build AES designs with an emphasis on the S-box utility, resilient to PAAs, also ensuring minimal area and power overheads so as to be able to fit into the resource constraint IoT devices. For the assessment of the constructed design, this work undertakes a full proof assessment on Application Specific Integrated Circuit (ASIC) and Field Programmable Gate Array (FPGA) platforms to evaluate hardware security metrics like MTD, SNR, MI,and TVLA.

The contributions of this thesis are organised into five major chapters. The following Chapter 2 undertakes an investigation to trace which S-box out of the state-of-the-art designs offers the least area and power, and also offers the best security. The hardware costings are estimated through ASIC synthesis using UMC 65 nm technology node, and the security metrics evaluated on SASEBO.

Chapter 3 analyzes the AES' modes of operation defined by NIST, namely, Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB), Output Feed Back (OFB) and Counter (CTR), and proposes a novel mode offering better security than the existing standard modes. The hardware resources of the proposed mode are also optimum in comparison to the existing ones.

Chapter 4 highlights a new scheme of offering side-channel security by splitting the SubBytes round operation over multiple clocks to implement the 16 S-boxes, instead of a single-clock operation. The SubBytes is executed over 1 clock, 2 clocks, 4 clocks, 8 clocks and 16 clocks to assess the offered security, resulting in 12-clock, 22-clock, 42-clock, 82-clock

and 162-clock AES design implementations. The 82-clock design is modified to incorporate the SubBytes implementation by utilizing the negative clock edge, resulting in the highest security among other investigated cases, in addition to optimum hardware expenses.

Having boosted the intrinsic resilience of AES without actually adding a countermeasure by adopting the strategies in the aforementioned chapters, Chapter 5 proposes a nanoscale countermeasure in the form of a compression and expansion Random Number Generator (RNG) aided with buffer-based delay. This proposal is implemented in addition to the intrinsic measures in order to have negligible area and power overheads, without compromising on AES' attack resilience.

Finally, Chapter 6 draws a conclusion out of the works carried out, and sheds some light on the possible future works ahead.

CHAPTER

2

LITERATURE SURVEY

Contents

2.1 AES design strategies befitting IoT hardware resources constraints 18
2.2 Countermeasure attempts to secure AES designs 27
2.2.1 Hiding-based countermeasures 28
2.2.2 Masking-based countermeasures 41

This thesis chapter takes a ride through various S-box design strategies developed after discovery of AES in 2001. Mathematicians laid down strongly confusing steps for the final and intermediate data to be unrelated to the original one. However, the design did not take into account the fact that upon building a circuit for the same, it may leak some significant information in the form of power side-channel leakage. In order to thwart these attacks, countermeasure mechanisms also have been endeavored parallelly, however things are coming into the light only after the emergence of IoT in the communication arena. The IoT edge devices being physically accessible suffer from a huge threat of such attacks. With this in mind, a two-decade survey of countermeasures is also presented in this chapter.

2.1 AES design strategies befitting IoT hardware resources constraints

The CPA attack model targets the S-boxes in the SubBytes and the discussed security metrics classify them as resilient to attacks or not. Also, with the SubBytes unit consuming 75% of the total AES power consumption and IoT edge environment being resource constraint, a detailed analysis of the S-boxes becomes hugely significant. The chronological development of S-boxes based on their design target is presented below:

Low gate count / small area-based

Rijmen, one of the inventors of AES, was aware of the hardware complexities to be involved in $GF(2^8)$-based calculations [19]. Hence, he himself proposed expressing an element of $GF(2^8)$ as a polynomial of degree 1 with coefficients from $GF(2^4)$. The task of calculating multiplicative inverse in $GF(2^8)$ was transformed to calculating the inverse in $GF(2^4)$ with some multiplications, squarings, and additions performed in the reduced $GF(2^4)$. No hardware design was carried out in regard to this proposal. However, Lin et al. [20] depicted its hardware design and fabricated it on-chip, a year later, providing an area efficient implementation.

Improving upon Rudra et al.'s work [21], Satoh et al. [22] recommended further optimization of S-box by announcing a new composite field $GF(((2^2)^2)^2)$. It utilized a 3-stage method of initially mapping all the elements of field A to composite field B using an isomorphic function, then computing the multiplicative inverses over field B, and, finally, re-mapping the computation results to A.

Unlike Rudra et al. [21], which implemented the whole AES round transformations in the composite field $GF((2^4)^2)$, Wolkerstorfer et al. [23] implemented only the S-box operations in $GF((2^4)^2)$, using polynomial basis. Their design merged encryption and decryption S-boxes in order to use multiplicative inversion circuit for both the operations.

Lu et al. [24] proposed the idea of integrating the AES encrypter and decrypter to achieve tremendous hardware savings. This work targeted to improve upon the LUT method of implementing S-boxes, named as inverse-optional S-box module.

Mentens et al. [25] attempted to improve upon Satoh's S-box [22] by designing another $GF(((2^2)^2)^2)$-based implementation. Mathematical investigations were made to find better candidates for: i) irreducible polynomials used to create extension fields and (ii) transformation matrices that enable mapping of elements from one representation to the other.

Canright [26], too, improved upon Satoh et al.'s S-box [22] by proposing three optimizations- choice of representation of polynomials, common subexpressions elimination,

and logic gates optimization. In the first optimization, 432 possible cases were investigated considering all the sub-field polynomial and normal bases.

Boyar et al. [27] [28] reduced the gate count of Canright's S-box [26] from 120 to 113 gates by reducing the non-linearity of a circuit (defined by the number of non-linear gates it comprises of) and reducing the number of gates in the linear components of the already reduced circuit. Contrary to a full-fledged circuit, this work presented only an experimental proof of concept, and synthesis results, too, did not reflect much improvement [29].

Ueno et al. [30] made an effort towards compact and efficient S-box implementation in the tower field $GF((2^4)^2)$, based on a combination of non-redundant and redundant GF arithmetic. Their recommended design utilizes redundant GF representations, namely, polynomial ring representation (PRR) and redundantly represented basis (RRB), to implement $GF(2^8)$ inversion using a tower field $GF((2^4)^2)$.

Jean et al.[31] tried to reduce the gate count in Canright's S-box (without exploring different sub-fields) by introducing the bit-sliding technique which makes the datapath bits slide, thereby reducing the datapath from s-bits to a single s-bit.

Masoleh et al. [29] proposed an S-box architecture in $GF((2^4)^2)$, which comprised of the input and output transformation blocks and the composite inversion field block which was further sub-divided into three sub-blocks: exponentiation block, subfield inverter, and output multipliers. A minimal number of gates in the transformation matrices was obtained by solving the shortest linear program (SLP) problem. Building upon this work, they developed a smaller and faster combined S-box [32] in the tower field $GF(((2^2)^2)^2)$ using normal basis.

Maximov et al.'s work [33] holds the record for the least gate-count-based design for both forward as well as combined S-boxes. Based upon Boyar et al.'s design [27], this work considered various methods and techniques to find the smallest circuit. The effort involved realizing a given linear transformation on n-input signals and m-output signals, bound by a constraint of a maximum depth, maxD, of the circuit.

High-speed-based

Rudra et al. [21] initiated the study of composite-field techniques by performing all the AES operations in composite field $GF((2^4)^2)$ utilizing the polynomial basis. Bitslice technique [34] was employed for the circuit design for both software and hardware implementations. Satoh et al.'s implementation [22] targeted high throughput, too, apart from small area.

Kuo et al. [35] exploited the LUT-based method in designing a high-speed S-box. Verbauwhede et al. [36] observed the area-latency trade-off curves for direct implementation of S-box using LUTs, with the composite field implementation of Wolkerstorfer et al. [23] and found the direct implementation method faster. Targeting a high-throughput design, they designed the first hardware circuit for AES on silicon using an LUT-based S-box. Another AES implementation on-chip by Hodjat et al. [37] based on the same technology utilizing an LUT-based S-box was made to boost the throughput. Although it succeeded in doing so, the improvement was made in MixColumns rather than the S-box.

Morioka et al. [38] presented the first high-speed S-box design without utilizing the conventional GF-based or LUT-based methods. It employed a twisted binary decision diagram (BDD) [39] and the T-box method [40] to boost the speed. The twisted BDD architecture involves a parallel arrangement of 8 BDDs, each corresponding to a primary output.

The area-efficient AES design by Lin et al. [20] utilizing Rijmen's proposal [19] for S-box optimization also achieved a high throughput using pipelined techniques. A suitable basis was chosen for transformation between $GF(2^8)$ and $GF(2^4)$.

Hodjat et al. [41] pushed the envelope for high throughput designs by employing loop unrolling and inner-pipelining techniques. Composite field implementation of $GF(2^8)$-based S-box over $GF(2^4)$ operators suffers a long critical path, thereby reducing throughput.

Rudra et al. [21] implemented all the AES rounds in the composite field $GF((2^4)^2)$; however, they did not depict proper hardware circuitry for the same. Mathew et al. [42] [43] presented hardware circuits for the S-box and the whole AES in the same fashion and coined it as native $GF((2^4)^2)$ composite field design.

Batina et al. [44] employed genetic algorithm (GA) for the first time in order to find the most efficient way of pipelining an S-box to increase its throughput. A polynomial basis S-box implementation in $GF(((2^2)^2)^2)$ used by Satoh et al. [22] and Mentens et al. [25] was considered, and GA deployed to find a good solution for positioning the pipeline FFs to reduce the critical path as much as possible.

Wang et al. [45] proposed a block-level in-memory architecture for AES design. In this method, non-volatile domain wall (DW) nanowire devices were employed instead of using the conventional SRAM LUT. The 8-bit results were split into distinct nanowires to accelerate the nonlinear transformation.

Masoleh et al.'s work [29] describing small area design also provided high throughput for the forward and combined S-boxes. Similarly, the record smallest design by Maximov et al. [33] also holds the record for the highest throughput obtained for an S-box.

Low-power-based

Morioka et al. [46] presented the first S-box/AES design targeting low power at the logic/gate level. Conventional S-boxes suffer from large power consumption owing to complicated signal path problems. A low power 3-stage method Positive-Polarity Reed-Muller (PPRM) [47] architecture was designed in which the gates were arranged, so that: (i) dynamic hazards are avoided by ensuring the signal arrival times at the gates are as close as possible, and (ii) the propagation of dynamic hazards is avoided by placing the hazard-transparent XOR gates after other gates.

Bertoni et al. [48] attempted to improve the energy-efficiency of conventional LUT-based S-box design. A one-hot representation of the S-box elements was chosen with increased input and output lines and synthesis of a $2N \times 2N$ function. The proposed circuit reduced the average energy consumption associated with transitions on the primary inputs at the cost of an area penalty.

Wolkerstorfer et al.'s work [23] was reused by Feldhofer et al.[49] to obtain a low-power, small die-size implementation of AES "on-chip". In this work, the S-box was modified slightly by inserting a pipeline register in order to shorten the critical path and lower glitching activities. A low-power design with a lesser area than Satoh [22] & Pramstaller [50] was attained, ignoring throughput considerations (only 9.9 Mbps).

Liu et al. [51] presented the first-ever full-custom S-box design using Pass Transistor Gate (PTG), working on Wolkerstorfer's design [23]. A PTG-based latch was used to prevent the propagation of dynamical hazards in the S-box. The PTGs were used to design low-power XOR gates which were the major building blocks of Wolkerstorfer's design. Ahmad et al. [52] reused this idea to design a novel 2-input XOR gate using pass-transistor logic (PTL) and utilized it in the S-box, which proved to be a breakthrough in low-power S-box designs. This design stands to be the least power-consuming one.

The concept of native $GF((2^4)^2)$-based composite field S-box design [43] was reused by Mathew et al. [53] themselves to attain a low-power AES implementation. They built an on-die lightweight nano-AES hardware accelerator targeting mobile SoCs.

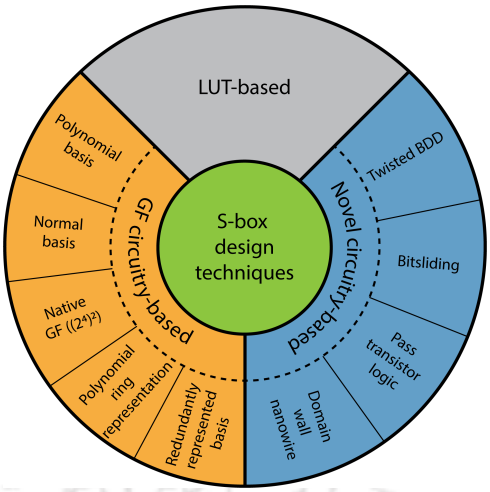


Figure 2.1: Classification of S-box design principles

Efficiency-based

Efficiency, defined by area-delay product (ADP), has been a neglected parameter in S-box designs. Ueno et al.'s low gate count design [30], utilizing a combination of redundant and non-redundant representation of polynomials, also reported being an efficient one. In contrast to non-redundant representations, redundant representations provide a wider variety for the selection of modular polynomials. This flexibility allows efficient isomorphic mappings from/to $GF(2^8)$.

However, Masoleh et al.'s design [29], which holds the record for the smallest area, asserts their design to be the most efficient. They conducted an exhaustive evaluation of each and every block in the S-box circuit, using both structural and behavioural modelling to reach the synergy between theoretical algorithms and technology-supported CAD tools. The structurally modelled circuit provided the most efficient S-box implementation.

Comparative Analysis of the S-Boxes

Various design techniques were employed to achieve the S-box design targets. Apart from the conventional methods like LUT and GF-based circuitry, some novel circuitries were also seen. Although a majority of the designs were synthesized for ASIC simulations, few of them were implemented on-chip. The design principles can be categorised according to the representation shown in figure 2.1.

The classification depicts three broad design techniques as already discussed. It is an established fact that the LUT-based technique is the most basic way of designing an S-box. In the GF-circuitry-based technique, polynomial ring representations and native $GF((2^4)^2)$-based designs were developed from the conventional polynomial and normal basis representation of polynomials. The novel circuitry-based S-box designs employed new digital circuits and principles to realize the operations involved in the implementation of an S-box rather than opting for the conventional LUT-based or GF-based circuit designs.

The hardware results of the designs discussed in the previous section are presented in table 2.1, with their gate count, area, maximum frequency of operation, throughput, and power, along with some remarks for every design. Before analysing the table, it must be noted that not all S-box designers reported the results in terms of its hardware resources utilisation. S-box, being a component of AES, some designers reported results on the basis

of AES' hardware resources utilization. The same is highlighted by shaded gray in the table. The entries in the table are enumerated in order of their discovery in the literature.

From the table, we can infer that most of the S-box designs have been carried out utilizing the polynomial and normal basis representation of the polynomials barring some conventional LUT-based designs. The composite field arithmetic designs utilizing polynomial and normal basis have explored both $GF((2^4)^2)$ and $GF(((2^2)^2)^2)$-based implementations to the fullest. Different irreducible polynomials and isomorphic mappings to map elements of $GF(2^8)$ to the composite fields have also been widely studied [54]. Only some designs have been made using different VLSI design principles like the BDD-based, PTG-based, nanowire-based, or bit-sliding-based architectures. From the remarks column, it can be figured out that initial S-box designs focussed on smaller gate count and area. However, high throughput and power minimization seemed to be of some interest gradually. Finally, owing to demands from IoT devices, the research clocked back to a smaller gate count design. In terms of the design techniques, as laid down by Canright in 2005 [26], normal basis seems to provide smaller designs than polynomial basis.

In terms of gate count, as claimed by Maximov et al. [33], their design seems to provide the least gate count for S-box. Consequently, the smallest area design can be credited to them. Although we may see a difference of only 18 gates with respect to Canright's design [26], it becomes appreciable only when we realize that an S-box is utilized 200 times in encrypting one plaintext ($16\times10 = 160$ times in 10 round operations and $4\times10 = 40$ times in key-scheduling operations). Thus, in total, a substantial amount of 3600 gates can be saved using Maximov et al.'s design [33] for one AES run.

The maximum frequency in which S-box can be operated on-chip can be inferred from Mathew et al.'s design [43] which showed a 2.1 GHz operable design. The ASIC synthesis, however, depicted a 780 MHz design by Morioka et al. [55] as the highest frequency of operation. These designs also permit the highest frequency on-chip implementation and ASIC synthesis of the AES design as a whole at 2.1 GHz and 909 MHz, respectively.

Throughput in the literature has mostly been reported for the whole AES design and not S-box in particular because apart from its dependence on the finite-field arithmetic based circuits, it relies heavily on the key-scheduling architecture as to whether the keys are generated on-the-fly or are pre-computed. As this work is based on an investigation of S-boxes alone and not AES designs, the author does not assert the highest throughput AES design. However, Mathew et al.'s work [43] achieving 53 Gbps on-chip and Hodjat et al.'s work [56] achieving 30-70 Gbps in ASIC synthesis can be regarded as some of the best throughput-based designs in the literature. The nanowire-based AES made a huge leap in throughput by achieving an enormous figure of 224 Gbps.

With reference to power consumption, it is evident that this parameter has been less explored. Ahmad et al.'s novel low-power XOR gate-based S-box design [52] seems to be the best amongst low-power candidates. For the AES implementation, the bit-sliding technique [30] seems to consume the least power. Another design parameter that has received very less attention is 'efficiency'. Masoleh et al.'s design [29] is the most efficient one overpowering Ueno et al.'s design [30].

Energy, another critical design parameter, has been completely overlooked, often confusing it with power. Energy consumption per operation is the optimisation goal for battery-powered devices. This implies that the power-delay product should be minimised. In contrast, for passively powered devices, the mean power consumption is of significance; the duration of the operation is inconsequential. In spite of the large total energy consumption, the power consumption clock cycle is limited.

Table 2.1: S-Box (AES) Hardware Resources Utilization

Reference	Tech. (μm)	Design Technique	#Hardware	Area (μm^2)	Max. freq. (MHz)	Throughput (Gbps)	Power (μW)	Remarks
[21]	S/W	Normal basis: $GF((2^4)^2)$	- 256k gates	- -	- 32	- 7.5	- -	Proposed the use of composite field arithmetic where the whole AES round operations were performed in $GF((2^4)^2)$. Bitslice technique was used in the overall AES implementation.
[22] (merged) (speed optimized)	0.11	Polynomial basis: $GF(((2^2)^2)^2)$	294 GEs 21.337k GEs	- 205	271 224.22	- 2.6	- -	Compact and high-speed design presented using a new composite field $GF(((2^2)^2)^2)$. One cycle per round version provides highest throughput.
[22] (merged) (area optimized)	0.11	Polynomial basis: $GF(((2^2)^2)^2)$	294 GEs 5.398k GEs	- 52	271 131.24	- 0.311	- -	Upon using composite field S-box implementation in $GF(((2^2)^2)^2)$, area occupancy reduced to one-fourth the size of one using LUT-based S-box.
[23] (no pipelining)	0.6	Polynomial basis: $GF((2^4)^2)$	406 GEs -	108k -	70 -	- -	- -	A small area design implemented where only the S-box is implemented in $GF((2^4)^2)$ and rest of the operations in $GF(2^8)$.
[23] (pipelined)	0.6	Polynomial basis: $GF((2^4)^2)$	500 GEs -	120k -	125 -	- -	- -	Increased maximum frequency of operation at the cost of extra hardware resources, due to insertion of extra flip-flops.
[24]	0.25	LUT-based design	789 gates 31.957k gates	- -	- 100	- 0.609	- -	Low gate count design accomplished where common table of multiplicative inverse used for S-box and inverse S-box.
[55] [38]	0.13	Twisted BDD architecture	2815 GEs 167.556k GEs	- -	780 909	- 11.6	- 1.92M	A high throughput design supporting all encryption modes. T-box used to enhance throughput.

2.1: AES design strategies befitting IoT hardware resources constraints

Reference	Tech. (μm)	Design Technique	#Hardware	Area (μm^2)	Max. freq. (MHz)	Throughput (Gbps)	Power (μW)	Remarks
[46]	0.13	Polynomial basis: $GF(((2^2)^2)^2)$	712 GEs -	- -	10 -	29 -	- -	Performed the first low power AES design implementation, employing PPRM architecture.
[20]$^{\$}$	0.35	Normal basis: $GF((2^4)^2)$	762.67 GEs 58.43k GEs	- -	- 200	- 2.381	- -	An on-chip implementation of AES utilising GF-based S-box designed for high throughput and area efficiency.
[36]$^{\$}$	0.18	LUT-based design	- 173k gates	- 3.96	- -	- 1.6	- 56k	First on-chip implementation of AES utilising LUT-based S-box designed for high throughput.
[56]	0.18	Polynomial basis: $GF((2^4)^2)$	- -	- -	- -	- 30-70	- -	An area-throughput trade-off AES design using pipelined S-box.
[25]	0.18	Polynomial basis: $GF(((2^2)^2)^2)$	272 -	- -	- -	- -	- -	Low gate count design with 6 XOR gates lesser than Satoh's S-box [22].
[49]$^{\$}$	0.35	Polynomial basis: $GF((2^4)^2)$	- 3400 GEs	- -	- 80	- 0.009	- 4.5	Employed Wolkerstorfer's S-box [23] targeting low die size and low power.
[26]	0.13	Normal basis: $GF(((2^2)^2)^2)$	180 GEs (120 gates) -	- -	- -	- -	- -	Low area/gate-count design exploring 432 possible cases of S-box design using polynomial and normal basis in the composite field $GF(((2^2)^2)^2)$.
[26] (merged)	0.13	Normal basis: $GF(((2^2)^2)^2)$	234 GEs (152 gates) -	- -	- -	- -	- -	A single $GF(2^8)$ inverter allows computation of S-box and its inverse in the merged form, reducing the overall hardware consumption.
[37]$^{\$}$	0.18	LUT-based design	- -	- 0.79	- 330	- 3.84	- 54k	High throughput design suitable for both feedback and non-feedback modes of operation.
[57] (area-based)	0.13	Normal basis: $GF(((2^2)^2)^2)$	- 3.1k GEs	- -	- 152	- 0.121	- 37/MHz	8-bit datapath employed to obtain a compact design.

Reference	Tech. (μm)	Design Technique	#Hardware	Area (μm^2)	Max. freq. (MHz)	Throughput (Gbps)	Power (μW)	Remarks
[57] (power-based)	0.13	Normal basis: $GF(((2^2)^2)^2)$	- 3.2k GEs	- -	- 130	- 0.104	- 30/MHz	Power consumption minimized due to reduction in width of datapath, lower cycle count, and lower clock frequency.
[57] (speed-based)	0.13	Normal basis: $GF(((2^2)^2)^2)$	- 3.9k GEs	- -	- 290	- 0.232	- 62/MHz	Parallel operations carried out in AES implementation leading to low cycle count and high throughput.
[51]	0.25	Polynomial basis: $GF((2^4)^2)$	- -	8,744 -	- -	- -	140 (@10 MHz) -	First full-custom S-box design for low power using PTG.
[43]$^{\$}$	0.045	Native $GF((2^4)^2)$	- 416k transistors	759 0.15	2,100 -	- 53	- 125k	First on-chip implementation of $GF((2^4)^2)$-based design for high throughput.
[52]	0.065	Polynomial basis: $GF(((2^2)^2)^2)$	- -	288 -	125 -	- -	0.09 -	Full custom low power design using novel XOR gate. A throughput of 1Gbps achieved.
[44]	0.13	Polynomial basis: $GF(((2^2)^2)^2)$	725.25 GEs -	2,901 -	- -	- -	- -	High throughput of 3.07 Gbps obtained using pipelining with genetic algorithm determining position of pipelined FFs.
[53]$^{\$}$	0.022	Native $GF((2^4)^2)$	- 1.947k gates	- 2.2	- 1,133	- 0.507	- 13k	First reported low power design using asymmetric polynomials for encryption and decryption.
[30]	0.065	PRR and RRB using a tower field $GF((2^4)^2)$	332 -	- -	- -	- -	132.58 -	Efficient S-box design utilizing a combination of non-redundant and redundant GF-arithmetic, with an ADP of 1052.44.
[45]	0.032	Domain-wall nanowire-based	- -	- < 2	- 30	- 224	- -	High throughput and energy efficient design using pipelining methods, with an insignificant area overhead. Domain-wall nanowires reduce leakage power.

Reference	Tech. (μm)	Design Technique	#Hardware	Area (μm^2)	Max. freq. (MHz)	Throughput (Gbps)	Power (μW)	Remarks
[27]	-	Linear-circuit optimization	113 gates -	- -	- -	- -	- -	Formulated a straight-line program using 81 XOR/XNOR & 32 AND gates. Only proof of concept developed.
[31]	0.13	Bit-sliding	- 1560 GEs	- -	- -	- -	- 0.823	Low gate count design avoiding usage of many scan FFs. Not the best choice for battery-driven devices.
[31] (merged)	0.13	Bit-sliding	- 1738 GEs	- -	- -	- -	- 0.852	The last seven regular FFs replaced by scan FFs for the merged architecture.
[29] (lightweight)	0.065	Normal basis: $GF((2^4)^2)$	182.25 -	379.08 -	- -	- -	38.085 -	Small area S-box design using both structural and behavioral modelling with an ADP of 218.28.
[29] (fastest)	0.065	Normal basis: $GF((2^4)^2)$	208 -	432.64 -	- -	- -	42.750 -	Fast and most efficient S-box design using purely structural modelling with an ADP of 162.177.
[32] (merged)	0.065	Normal basis: $GF(((2^2)^2)^2)$	244.25 GEs (150 gates) -	508.04 -	862.81 -	- -	55 -	Employed a new tower field resulting in more compact transformation blocks after investigating 512 mapping circuits.
[33]	0.022	Normal basis: $GF(((2^2)^2)^2)$	195.10 GEs (102 gates) -	- -	- -	- -	- -	Number of heuristic and exhaustive search methods used to obtain the smallest design till date.
[33] (merged)	0.022	Normal basis: $GF(((2^2)^2)^2)$	253.35 GEs (127 gates) -	- -	- -	- -	- -	Fastest combined S-box till date using novel technique of "floating multiplexers". Two different linear matrices (forward and inverse) combined using the multiplexers.

[$] On-chip implementation **NOTE**: GE denotes gate equivalent

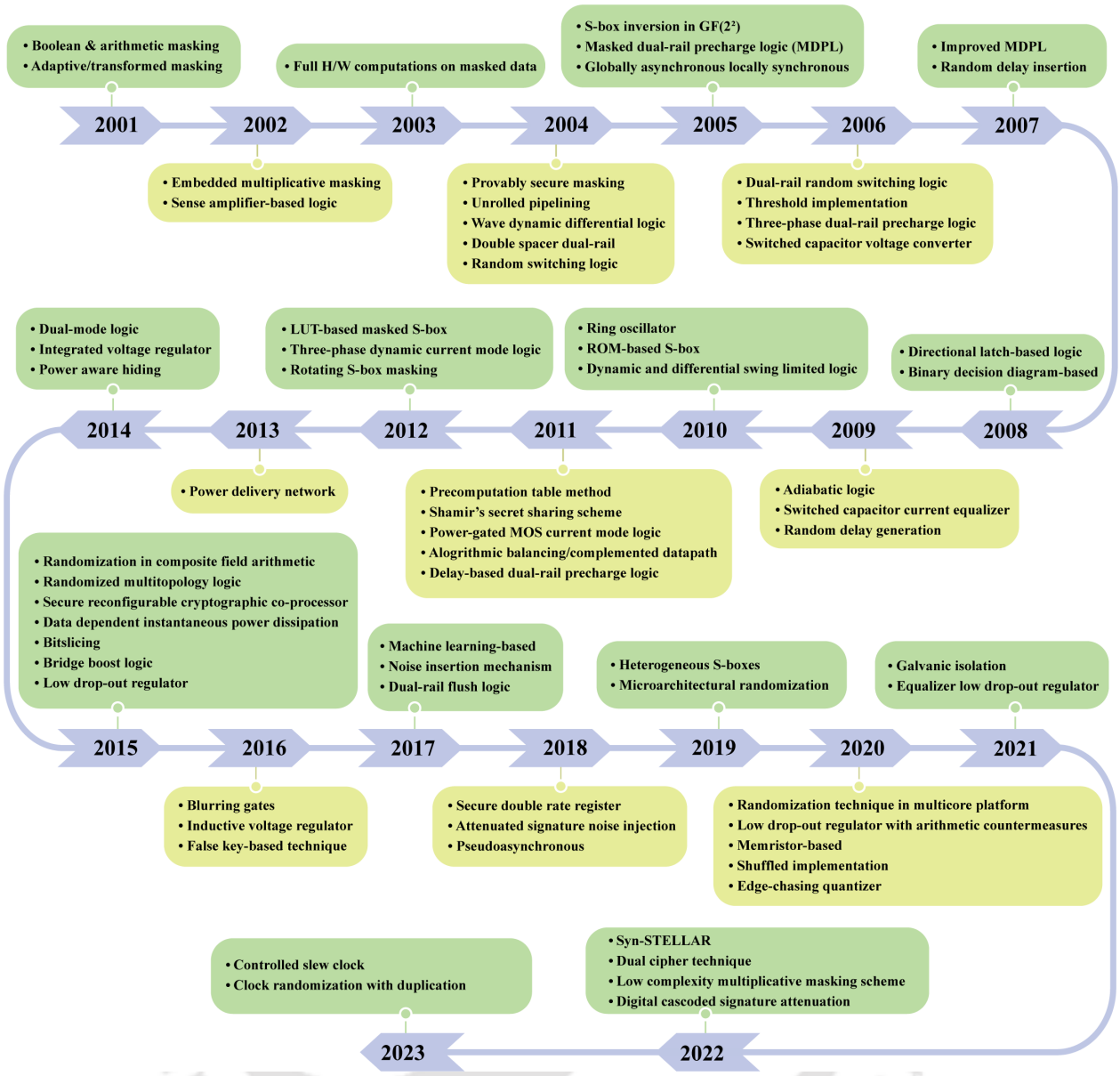


Figure 2.2: Year-wise depiction of countermeasures

2.2 Countermeasure attempts to secure AES designs

The study of various S-box design techniques was critical from the perspective of its resources' consumption since IoT environment is quite constricted. Apart from fulfilling the resources' perspective, an AES design also needs to deliver the required 'security'. With PAAs rendering AES unsafe, an extra circuit called the 'countermeasure' is attached alongwith, to amplify its resilience. Such an additional endeavor although boosts the resilience, however, taxes on area, power and performance of the design. An AES design with a countermeasure incorporated is called 'protected' whereas a design bereft of it is termed 'unprotected'. The prime purpose of a countermeasure design is to disrupt the power signature presented by an unprotected AES design. With its incorporation, the power trace pattern is disrupted and intrinsic properties altered so as not to be carrying any or carrying minimal information about the internal cryptographic operations.

This section wades through various countermeasure designs since the discovery of power

analysis attacks in 1999, as represented in figure 2.2. The study emphasizes on the area, power and performance overheads owing to the countermeasure, apart from signifying the security provided by each countermeasure in terms of MTD. The countermeasures are broadly classified as hiding or masking, which are elucidated as under.

2.2.1 Hiding-based countermeasures

The goal of hiding-based countermeasures is to subside the interrelation between the power consumption of cryptographic devices and intermediate values of the executed cryptographic algorithms by unsettling the relation between the power consumption of the devices and the processed data values. Hiding uses two different approaches to achieve the goal.

I) Random power-based hiding countermeasures

In this approach, the construction of the device is in a manner that the power consumption is random, i.e., a random amount of power gets consumed in each clock cycle. Primarily, the operations of the cryptographic algorithm are performed at different time instants during each execution. Following are some countermeasures which belong to this category.

Unrolled pipelining The success of a DPA attack against a rolled implementation of AES is due to the predictable nature of most registers with one round implementation. Ors et al. [58] proposed that using an unrolled and pipelined implementation of AES enables the inner rounds to act as noise generators, thereby making only the outer rounds partially predictable.

Random delay insertion Bucci et al. [59] proposed the random delay insertion technique, which utilizes a generic pipeline stage in the AES implementation where two registers provide cladding to a combinational network allowing delayed inputs to the combinational hardware by a random time, Δ_i, where, $i = 1, ..., N$. This produces two effects: variance on the output current waveform and decorrelation of charge transfer in a clock cycle from the processed data owing to the modified interval sequence of transitions induced by the input delays.

Switched capacitor voltage converter Telandro et al. [60] first secured smart cards from power analysis attacks by utilizing voltage regulators as a countermeasure. Taking hints from their work, Uzun et al. [61] developed a new power management technique as countermeasure called the converter-gating (CoGa). Individual stages of an interleaved switched-capacitor are turned on and off by a stage-control run by a PRNG, depending on the workload information.

Although CoGa tries to scramble the power consumption profile by injecting additional spikes, the device is still vulnerable because of the pattern of activation/deactivation depending on the workload demand. CoGa technique also breaks down if an attack is performed with no large enough changes in the load current demand capable of triggering CoGa to activate/deactivate interleaved stages. Also, the correlation between input and actual current profile is still expected even if CoGa is triggered since the activation/deactivation occurs in accordance with a change in workload demand.

Yu et al. [62] adopted converter reshuffling (CoRe) to scramble the input current profile during insufficient load current change to turn on or off a converter stage. A PRNG juggles the active and inactive converter stages by concurrent gating some active stages while turning on the same number of inactive stages under constant load current demand. The CoRe

technique is insensitive to converter-gating and does not depend on the load current demand to trigger it. The advantages of CoRe operation are the disruption of input current profile while turning on and off different converter stages and the exhibition of different current signatures owing to a variance of the phase of active converter stages.

The same research group reported that attackers can obtain the regulator's phase information and switching frequency, f_s, by using machine-learning (ML) [63]. As a solution, they proposed a time-delayed CoRe technique in which half of the converter stages are delayed by a certain time shift to eliminate possible synchronization. They also proposed using two PRNGs to resolve the synchronization issue [64].

The aforementioned works utilizing voltage regulators (VRs) used power trace entropy (PTE) as a security metric; however, [65] investigated centralized and distributed implementations of the CoRe regulators and examined how the correlation coefficient would be affected by the physical placement of VRs. For the AES with 16 S-boxes, 16/N number of phases can be utilized using a distributed CoRe architecture to scramble the side-channel power. However, a centralized CoRe architecture availed utilization of all the phases to scramble the input power consumption.

Random-delay generation (RDG) A random software delay is a piece of code, like a dummy loop, in order to prevent the knowledge of the program at a particular moment in time. Tunstall et al. [66] suggested modifications in the distribution of an independently generated random delay to ensure an increase in the variance of the sum and a decrease in its mean. However, Coron et al. [67] proposed a floating-mean-based RDG with the idea of generating non-independent random delays to obtain a greater variance of the cumulative delay for the same mean. They found out that the floating mean method for random delay generation exhibited compromised security for improper choice of parameters. They suggested an improved floating method [68] where a random integer is chosen before each new execution to have a wider choice of parameters, maintaining the efficiency of the implementation.

Ring oscillator Liu et al. [69] proposed a countermeasure comprising digital controlled ring oscillators mounted on the S-box, thereby evading any extra delay in the critical path. The ring oscillators are enabled or disabled, leading to changes in the power consumption characteristics. Random masks can also be generated using an internally designed random generator. However, the generated random bytes turn out to be the same once the system is reset.

The same authors troubleshoot the reset problem in [70] by incorporating a true random number generator (TRNG) and self-generated true random sequence. They extended this work in [71], where an effort was made to reduce the overhead by employing ring oscillators in Fibonacci and Galois configurations to generate the random sequence.

Nassar et al. [72] also utilized the ring oscillators, however with a dual purpose. They were used to detect the occurrence of an attack along with a detection sensor, and also to generate noise to hide the effects of the secret intermediate outputs on the device's power consumption. In the attack detection mechanism, the oscillators' frequency is observed for any change, which indicates the application of an attack. As a noise generation scheme, the oscillators are implemented with a runtime-configurable chain length which is constantly adjusted to a new random value, thereby altering the noise frequency. A simple frequency filter is bound to fail separating the noise contributed by different frequencies.

Power delivery network (PDN) Wang et al. [73] performed a novel investigation to study the effect of the power grid on SCA and found results demonstrating the frequency-dependent SCA resistance due to PDN-induced noise. The RLC property of the power grid brings about a frequency-domain distortion on the supply current. This intrinsically limits any propagation of useful information to supply current, leading to a change in the supply current profile when it passes through the PDN from inside the chip to the external pin.

Dual-mode logic (DML) DML was originally proposed for energy performance optimizations [74], which basically comprise of a conventional CMOS gate and two additional clocked transistors. Such a gate allows operation in two functional modes: static and dynamic, which are determined by the clock signal. Upon randomizing these modes, the same data results in different random power profiles [75].

Integrated voltage regulator Kar et al. [76] first modeled and analysed the impact of an inductive integrated voltage regulator (IVR) on PAAs of encryption engines. The input current drawn by an IVR is the current observed by an attacker at the supply pins. This current is complex, frequency and logic dependent, thereby reducing the correlation between the generated and observed current traces.

IVRs are now integrated on the same die with processor cores by the processor power delivery community owing to their improved supply noise and ability to support fine-grain output voltage. IVR, essential for power management, comes with nearly zero overhead in terms of area/power/cost when additionally utilised to resist PAAs. Kar et al. [77], for the first time, exploited IVRs as a countermeasure core with a detailed time-domain and frequency-domain statistical analysis. Fully integrated voltage regulators (FIVRs) were designed with low passives (L & C), indicating enhanced protection by controlling loop delay and pole-zero locations of the compensator.

The same research group [7] demonstrated improved power attack resistance by utilizing an on-die all-digital high-frequency IVR for an AES core. The IVR comprises of a configurable digital PID controller, a digital discontinuous conduction mode (DCM) controller, and a loop randomization (LR) block. These components are utilized to augment attack resistance with nominal power/performance overheads while preserving adequate local voltage regulation and transient performance. In contrast to the supply current equalization method, the IVR alters the current signature of crypto-engine before the attacker measures it at the IVR's supply. Large signal transformations are achieved by using the inductive IVR power stage, regulated by the switching frequency, duty cycle, and inductor/capacitor values. Lastly, the possibility of alignment of traces at the attacker's end, is reduced by desynchronizing the AES operating clock and the IVR switching clock.

Singh et al. [78] further utilized IVRs and reported random fast voltage dithering (RFVD) enabled by an integrated inductive voltage regulator (IVR) and all-digital clock modulation (ADCM). Contrary to the conventional encryptions which are performed at a constant voltage and frequency, RFVD dithers the voltage around the target level using a high-frequency, high-bandwidth IVR with each encryption assigned a random different voltage. The correct operation and timing randomness are achieved in unison with the help of ADCM. Thus, RFVD achieves both amplitude and timing distortion of the generated power trace.

Kar et al. [79] used an IVR to alter current signatures generated by a crypto-engine. A loop randomizer, designed using an all-digital circuit block, randomizes the IVR transformations. The load current signatures generated by a digital logic and measured at the IVR's input are transformed by IVR, thereby shielding the internal supply node of the AES engine.

Low drop-out regulator (LDO) Conventional voltage-regulator-based approaches mainly concentrated on mixed-signal switching VRs that require embedded passives to enable power-attack protection [60] [61] [62] [76] [80]. A possible solution to this is the utilization of low-dropout regulators, which already are integral parts of the power delivery architecture of modern processors, to reduce the noise coming from power supply, manage power efficiently and improve performance. The integration of an LDO on an encryption engine shifts the point of attack from the supply of the encryption engine to the supply of the LDO. Singh et al. [81] investigated the usage of an all-digital low-dropout regulator (ADLDO) as a countermeasure against power analysis attacks. It introduces a small signal current transformation coupled with noise due to quantization and limited sampling rate in its control loop.

Singh et al. [80] performed the first case study on low drop-out regulator as a countermeasure, where an analog LDO's bandwidth was varied by modifying pole locations. However, no power analysis attack was reported. The same research group [82] [83] demonstrated power attack resistance using an on-die all-digital series low drop-out regulator. Perturbations are induced by the control loop in a baseline DLDO which are enhanced by a random switching noise injector (SNI). A power stage control with a randomized reference voltage (V-REF) generator and an all-digital clock modulation (ADCM) are utilized by the noise injector to generate the perturbations. The DLDO power stage acts as a low pass filter (LPF) whose bandwidth is governed by the equivalent resistance provided by the power stage and output capacitor leading to attenuation of high-frequency current signatures.

Singh et al. [84] and Deniz et al. [85] pointed out the susceptibility of digital LDOs for ultra fine-grained power management and load regulation point, owing to their simple design and scalability across process nodes. Singh et al. [83] reported another on-die security-aware LDO, which induces control-loop induced perturbations using a random SNI and an R-VREF generator coupled with all-digital clock modulation. A pseudorandom pulse for the SNI is generated every clock cycle in accordance with the DLDO, resulting in pseudorandom spikes throughout the supply voltage. A critical path replica (CPR)-based global modulator (GM) and a local modulator (LM) are used in an ADCM to respond to DC shift/transient noise in the supply voltage every cycle.

Kumar et al. [86] utilized a high-bandwidth non-linear LDO (NL-LDO) regulator in conjunction with some AES arithmetic countermeasures. The NL-DLDO regulator comprises of a non-linear controller and a power train with tunable-strength PMOS tiles. The regulator, provided with multiple knobs to optimize the sought resistance in the frequency domain, swiftly responds to the high-frequency transients. Three output comparators asynchronously trigger the non-linear control (NLC) loop at high, low, and under-voltage thresholds to regularly modulate the number/strength of active static/dynamic tiles. Finally, the NL-DLDO is connected with an AES engine with arithmetic countermeasures, such as randomized dataflow through heterogeneous S-boxes and masked MixColumns.

Randomization in composite field arithmetic The Galois-field arithmetic structure of S-boxes suggests that the three parameters $\{\phi, \lambda, \delta\}$ are not constant since there could be much more than one eligible isomorphism. Masoumi et al. [87] used a random isomorphism made by generating different sets of $\{\phi, \lambda, \delta, \delta^{-1}\}$, and a set is chosen randomly in each block encryption/decryption. The significance of GF-based mathematical background for S-box design can be comprehended from the fact that such modifications in the basis representations lead to improved security [88].

Randomized multitopology logic (RMTL) Avital et al. [89] proposed a new logic gate design called randomized multitopology logic. Such a gate is configured to work in one of several topologies, like static CMOS, conventional dynamic logic with precharge, conventional dynamic logic with predischarge, non-standard dynamic logic with precharge, and non-standard dynamic logic with predischarge. The same logic function is implemented by each topology, however, generating different power profiles.

Secure reconfigurable cryptographic co-processor (SRCP) Shan et al. [90] developed a means to configure the algorithm with multiple countermeasures using reconfigurable processing elements (PEs). The first countermeasure confirms idle PEs to execute random operations; the second one performs a partial complementary operation by sending a signal to a functional unit and its inverted signal to its complementary idle clock at the same time; the third one executes instructions out of order, and the final one inserts random dummy operations to avoid storing intermediate data of two consecutive rounds in the same register.

Data-dependent instantaneous power dissipation Levi et al. [91], for the first time, performed a study on intra-cycle power dissipation affected by data-dependency. The intra-cycle current is changed to increase randomness by using static and dynamic data-dependent hazards. A static hazard occurs when an unwanted pulse tampers with an output that should remain static, whereas a dynamic hazard changes the output multiple times before settling at the designated value. The same research group found that a poor delay assignment makes this prone to PAAs [92]. A delay assignment algorithm is designed by assigning proper data-dependent delays to hinder signal and multibit attacks.

Blurring gates Avital et al. [16] proposed the concept of blurring gates with a possible design using a standard CMOS library. Similar to RMTL [89], blurring gates, too, randomly select either of the two operations modes: static or dynamic (precharging or predischarging the output voltage). However, the difference lies in the fact that the BG units can be embedded in any desired path of the logic in the crypto-module. The BG units enable precharge/predischarge of only some randomly chosen nodes, unlike existing randomization countermeasures where all the nodes of the design are precharged/predischarged.

Noise insertion mechanism Yu et al. [93] investigated the implications of noise insertion mechanisms, such as additive non-white and multiplicative noise, as countermeasures. Non-white noise, such as extra power consumption and random power grids, and white noise, such as on-chip decoupling capacitor storing from and discharging to power supply, are the types of additive noise employed. On the other hand, multiplicative noise, such as random dynamic voltage scaling and frequency scaling are employed to scramble the power profile by randomly altering supply voltage or clock frequency.

Secure double rate register (SDRR) Countermeasure like random precharge logic (RPL) suffers from the drawback that it requires the combinational path to be duplicated. On the other hand, countermeasures, such as blurring gates and random delay insertion, secure the combinational logic with no effect on the power consumption drawn by sequential logic (i.e., registers), which forms a significant contribution to the total current composition, eventually information leakage.

In the quest to secure both the sequential and combinational parts of the implementation, Bellizia et al. [94] proposed the secure double rate register technique, which does away with the replication of combinational paths, thus reducing area and power consumption overhead. SDRR comprises two cascaded registers and an input multiplexer to enable the selection of input data of the first register. The conventional registers are replaced by SDRRs in which one of its registers stores a real input datum, whereas a random input datum is stored in the other one and vice versa. The selection between real and random data is performed based on a clock signal of the reference architecture, whereas another clock signal with doubled frequency is used by the SDRR flip-flops. Thus, the SDRR feeds correct and random data in an alternating manner.

Attenuated signature noise injection (ASNI) Das et al. [95] combined the noise injection and supply isolation countermeasure techniques. SNR of the leaked information, as observed by an adversary, is reduced by noise injection by suppressing the AES signature, whereas supply isolation, as the name suggests, decouples the supply from the encryption engine. A signature attenuation hardware is developed employing a shunt-LDO-based loop enabling simultaneous regulation of supply voltage for AES logic and supply current independent of the AES transitions.

Pseudoasynchronous GALS, which utilizes both synchronous and asynchronous design styles, suffers from a potential threat of having the operating frequency of the local block discovered. Hence, Levi et al. [96] proposed a pseudoasynchronous (pAsynch) design style where each bit is asserted with a different clock. Contrary to random sampling time, the clock cycles are changed in time based on the data processed. The current generated out of the switching activities while processing information is divided into small portions whose count depends on the current and previous values. These sub-divided portions are allocated in different time instants within the cycle period, thereby achieving hiding in the time-domain as well as amplitude-domain.

Microarchitectural randomization Singh et al. [80] revealed the susceptibility of sub-round architectures towards side-channel attacks. Dhanuskodi et al. [97] [98] built a register renaming architecture that randomizes the order in which the sub-round operations are executed without affecting the final output of the algorithm, also avoiding data hazards in the process. An enable generation circuit triggers the randomization of sub-round operations and a permutation stage after MixColumns. Rescheduling of the key expansion and key addition across the rounds also contributes to the randomization. The control signals generated by enable generator dictate the reading/writing of the state register in each computation cycle.

Randomization technique in multicore platform Random dynamic voltage and frequency scaling (RDVFS) is vulnerable due to the relation between frequency and voltage [99], and globally asynchronous locally synchronous (GALS) [100] incurs undue performance penalty due to the large exchange of data between the asynchronous blocks. Moreover, existing countermeasures, like the execution of instructions with dummy operations and random skipping of clock cycles, are considered ineffective as dynamic time warping has the ability to realign the power traces correctly even with the random clock frequency of the device.

Yang et al. [101] implemented Random task scheduling (RTS) and random insertion of operations (RIO) for multicore processors to misalign the power traces. Frequency and

phase randomization, and power state monitoring and control (PSMC) are employed in both time-dimension and amplitude-dimension to prevent the realignment of power traces. Also, a two phase locked loop (PLL) in GALS multicore architecture enhances the security with truly asynchronous operations.

Memristor-based Nanoelectronics-based countermeasure utilizing a memristor, was investigated for the first time by Masoumi [102] and found to be effective with minimal overhead. The difference between CMOS transistor and memristor is that the former is a bi-level circuit element, whereas the latter is a non-linear iso-input element. Thus, a non-linear power is drawn from the multi-level memristor device, thereby generating a staggering power profile.

Shuffled implementation Sasdrich et al. [103] and Patranabis et al. [104] attempted some shuffling-based countermeasures based on a limited number of processing order sequences. Harcha et al. [105] used a randomized sequence of bytes to reorganize the computation orders as well as storage locations. Using a dedicated permutation network, such as Benes network or Omega network, a sequence is generated for each clock cycle which limits the impact on the secured design's latency. The permutation network permutes a set of 16 constant values (0-15), and the generated random order gets stored in a memory which is used by the controller to drive the datapath.

Dual cipher technique Ciphers, C_1 and C_2 are called dual to each other if there exist invertible transformations, $f(\cdot)$, $g(\cdot)$ and $h(\cdot)$ such that

$$\forall P, K f(E_K(P)) = E'_{g(K)}(h(P)), \tag{2.1}$$

where P and K are the plaintext and cipher key, respectively. Zhou et al. [106] utilizes a sparse invertible matrix instead of the dense isomorphic mapping matrix for the transformations between the dual ciphers. Hence, the multiplications of the conversion matrix and other constant matrices involved in AES are simplified to a greater extent.

Controlled slew clock Ghosh et al. [107] pioneered to develop a controlled slewed clock by utilizing the inherent variability of CMOS digital circuits, easily compatible to any of the supply port countermeasure for multiplicative effect on PAAs' resilience. The controlled clock-skew helps to achieve variability in digital circuits which provides the effect of security. Primarily, the duty cycle gets distorted and slew-dependent latch delay varied as its effect. In addition, process dependent factors like location-dependent variability in Elmore delay and intra-die process variation (device mismatch) also get enhanced, leading to added security.

Clock randomization with duplication With [108] rendering clock randomization to be unsafe upon the usage of higher sampling frequency than the clock frequency of the implementation under attack, Moraitis et al. [109] coupled duplication along with the clock randomization technique. In the proposed architecture, two different randomized clocks are employed for two cryptographic cores, a primary, and a dummy. Both cores utilized different cipher keys to operate on the same plaintext resulting in disarrayed power traces. Synchronization, in this case, is extremely difficult as the portions of the trace resulting from the primary core and the dummy are not possible to be distinguished.

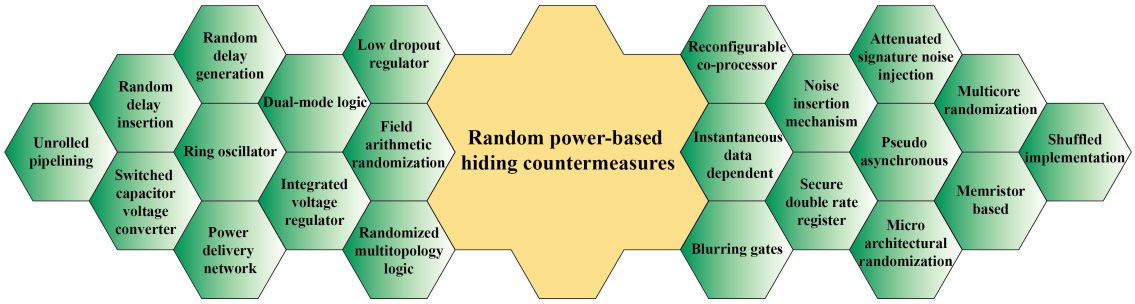


Figure 2.3: Random power-based hiding countermeasures

Thus, using these countermeasures, the power consumption of the device is randomized. A reduction in SNR is thus obtained by increasing the noise, making it difficult to perform successful attacks. All the investigated designs under the category of random power-based hiding countermeasures are collectively represented in figure 2.3.

II) Equal power-based hiding countermeasures

In this second approach of hiding, the device is built in a manner that all operations consume an equal amount of power in each clock cycle. This binding holds for all data values as well. This group of countermeasures affects the amplitude dimension of power traces. Some countermeasures which belong to this category are enumerated as follows.

Sense-amplifier-based logic (SABL) Tiri et al. [110] proposed the first hiding-based countermeasure in which a combination of dynamic and differential logic ensures an equal amount of energy consumption every clock cycle for all the four possible output transitions ($0 \rightarrow 0, 0 \rightarrow 1, 1 \rightarrow 0, 1 \rightarrow 1$). The input values are masked by differential logic ensuring energy dissipation when exactly one output node is discharged. With $0 \rightarrow 1/1 \rightarrow 0$ transition leading to additional power consumption than $0 \rightarrow 0/1 \rightarrow 1$, information leakage still persists. Dynamic logic is introduced to make the energy consumption independent of the input-switching pattern.

Wave dynamic differential logic (WDDL) The biggest disadvantage of SABL is that it requires a completely new standard cell library to be designed and characterized. The same research group, Tiri et al. [111] utilized standard building blocks to mimic the behavior of SABL gates by passing a wave of precharge signals to various stages of the combinational circuit. Unlike conventional precharging of the whole circuit altogether, the precharge signal in WDDL is rippled stage-by-stage, in accordance with SABL. The precharge wave can be launched by either inserting a precharge operator at inputs of the encryption module and outputs of the registers or by solely precharging the input signals of the encryption module.

Single-spacer dual-rail and double-spacer dual-rail Dual-rail code employs two rails allowing only two valid signal combinations, $\{01, 10\}$, to encode values 0 and 1, respectively. The switching protocol allows transitions from all-zeros $\{00\}$, a non-code word, to a code-word, and back to all-zeros, rendering monotonic switching. In order to balance the power signature, Sokolov et al. [112] used a dual-spacer protocol where two spacer states, i.e., $\{00\}$ for all-zeros spacer and $\{11\}$ for all-ones spacer, are used. In contrast to the single-spacer dual-rail, which mandates switching of the same gate/rail, the dual-spacer method switches

both the rails from the all-zeros spacer to all-ones spacer and back. Thus, all the gates forming dual-rail pairs are fired every computation cycle.

Guilley et al. [113] reported a security-related issue called 'early propagation effect (EPE)', in which a gate is enabled without waiting for the arrival of all its inputs. A possible way to avoid EPE is the insertion of buffers to balance the paths in a manner that every gate inputs arrive simultaneously. It is done using the spacers concept employing null conventional logic with null completion detection through the dual-rail signals (NCL-D). Sokolov et al. [112], in another set of work, proposed an arbitrary and random polarity of the spacer enabling switching of all the bits in each cycle of operation.

Random switching logic (RSL) Complementary operations equalizing signal transition frequency depends on wire length and fan-out, posing challenges to the designers. Suzuki et al. [114] proposed the RSL, which does not require complementary operations as it processes original signals and additional random signal simultaneously. The logic is based on two properties: the same 1-bit random value is utilized to execute masked operations for all input/output signals, and operations are executed while enable signal is 1, else driven to 0.

RSL requires custom-gate-based design, incurring high development cost, timing adjustment of enable signals, and a long design period. It halves the operating speed and doubles the hardware resources in comparison to an original AES circuit. Saeki et al. [115] proposed a new design methodology of RSL using standard cell libraries, called 'pseudo RSL'. In comparison to the WDDL scheme that needs an equal number of gates, the pseudo RSL attains better performances without reducing the operating frequency.

Globally asynchronous locally synchronous (GALS) Chapiro [116] was the first to present GALS, which was further used as a side-channel countermeasure by Gurkaynak et al. [100], aiming to combine the advantages of asynchronous and synchronous designs. A GALS module is constructed by enclosing a locally synchronous island with a self-timed wrapper which contains asynchronous port controllers and a local clock generator. A uniform power spectrum is produced by the asynchronous circuit due to the omission of global clock signal.

Three-phase dual rail precharge logic (TDPL) Bucci et al. [117] introduced a dual-rail precharge family called three-phase dual-rail precharge logic, which provides a scope of semi-custom design flow. It involves a three-phase operation with an additional discharge operation after precharge and evaluation. Both the output lines of a gate are charged to V_{DD} in the first phase (precharge), followed by one of the lines discharging to V_{SS} based on the input in the second phase (evaluation), and ultimately, the other line discharging too, in the final phase (discharge). Thus, the energy consumption remains constant over the operating cycle even if the capacitive loads are unbalanced.

Asynchronous directional latch-based logic (ADLBL) The major limitation of dual-rail designs is the dependence on matching capacitances which are practically tough to attain due to the sub-optimal nature of the routing tools in addition to the unavoidable manufacturing variations. Kulikowski et al. [118] proposed a design based on a dual-rail RTZ data communication protocol using a directional latch. The direction of discharge corresponding to both the rails is sensed by the latch and allows complete discharge of each dual-rail pair to maintain the appropriate logical value at the gate. Irrespective of the data, equal charging and complete discharging of both the rails are ensured for each cycle, ensuring an equal amount of total capacitance.

Dual-rail precharge with binary decision diagram (DP-BDD) Akishita et al. [119] proposed the DP-BDD architecture wherein a binary decision diagram forms the basis, which is a direct acyclic graph representing a Boolean function. AND-OR gates available in CMOS standard cell libraries are used to construct the DP-BDD. The architecture design ensures that the input signals always pass an equal number of AND-OR gates. This significantly reduces the EPE, a significant contributor to DPA leakage in WDDL.

Adiabatic logic-based The charge recovery logic family, like adiabatic logic, has been originally designed to reduce the circuit power consumption. Khatir et al. [120] exploited its usage in designing secure cryptographic circuits by decreasing the dynamic power consumption. This logic employs a DC bias voltage instead of ground at the source terminal of the NMOS transistors to eliminate non-adiabatic discharging of load capacitances.

Adiabatic logic was utilized to implement charge-sharing symmetric adiabatic logic (CSSAL) [121], which was further extended to design the S-box using multi-stage Positive Polarity Reed-Muller (PPRM) in [122].

Switched capacitor current equalizer Tokunaga et al. [123] [124] implemented a current equalizer involving integrated switch capacitors to isolate the encryption circuit from power supply. An array of capacitors ensures equal current drawn by the encryption core. The supply charges each capacitor, which facilitates the charging of encryption core while isolating it from the power supply. The capacitor is then discharged to a known constant voltage prior to recharging it to a level, ensuring equal amount of charge flowing from the external supply.

ROM-based S-box Conventional ROM operations involve selective pulling down of precharged bitlines based on the 'read' data word. Such an action leads to a data-dependent number of bitlines being discharged with some potential side-channel information being leaked. Teegarden et al. [125] proposed a ROM design which ensures the wordlines connection to the same number of devices and bitlines connection to the same number of gate capacitances, independent of the ROM data.

Dynamic and differential swing limited logic Renauld et al. [126] pursued an attempt to establish a switching activity independent AES implementation. It utilizes the dynamic and differential switching logic (DDSLL) [127] primarily used to realize the functionality of the gate. It mainly consists of a differential pull-down network (DPDN) working as a dynamic and differential self-timed low-swing logic offering low-power solutions. The dependency of power on the number of internal capacitances getting charged/discharged every cycle is minimized due to the construction of DPDN with Binary decision diagrams (BDD).

Power-gated MOS current mode logic (PG-MCML) MOS current mode logic (MCML) was introduced in 1992 [128] for high-speed and mixed-signal applications. The reduced voltage swing and differential operations offered by this logic are the two key elements in reducing the switching noise apart from frequency-independent power consumption. Cevrero et al. [129] utilized the properties of MCML and incorporated the power gating technique to reduce the static power consumption. Power switches and sleep transistors were inserted in the supply path to achieve the reduction. A constant bias current is generated by the current source, and an NMOS network is used to realize the Boolean function, which

drives the current to the load resistor. Thus, a power profile independent of input patterns or fan-out conditions is obtained. The standard cell design methodology proposed in [130] is used to design the PG-MCML gates.

Algorithmic balancing/Duplicated complemented datapath Verdier et al. [131] proposed a security strategy in which induced errors are detected and spread so that the resultant erroneous ciphertext doesn't lead to a successful DPA attack. The datapaths of round and key expansion blocks are duplicated to detect and check data consistency. The duplication follows a dual approach such that the original datapath works on the correct plaintext and key, whereas the duplicated datapath work on complemented values of the plaintext and key. In addition, the logic gates used in the datapaths are also complemented, i.e., XNOR gates replace XOR gates in the original datapath. Since HW/HD models [132] are used in DPA attacks, the complemented data approach balances the HW/HD leakage of power.

Delay-based dual-rail precharge logic (DDPL) Bucci et al. [133] developed a DPA-resistant countermeasure whose logic style relies on data encoding in the time domain. A complementary line is charged (evaluation) and discharged (precharge) once every clock cycle, and a datum is attached in accordance with a fixed delay between the complementary lines. The data encoding in DDPL is fully dynamic and is affected by leakage measurements, unlike standard-cell-based dual-rail precharge logic (DPL) and SABL, which is a semi-dynamic logic. This logic was later formalized as time-enclosed logic (TEL) [134].

Three-phase dynamic current mode logic (TPDyCML) Dynamic current mode logic (DyCML) gates, introduced by Allam et al. [135] are based on classical current mode logic gates with the advantages of high-speed and low noise. Mace et al. [136] were the first to employ it as a countermeasure, however, for a Khazad S-box. DyCML gates are made by combining a standard CML block, a dynamic current source, and a latch to store the result. Kim et al. [137] proposed a TPDyCML that eliminates the need for balancing wire capacitance of dual signals by using a three-phase configuration: charge, evaluation, and discharge phase.

Power aware hiding (PAH) Li et al. [138] introduced a special hiding technique which utilizes appropriate feedforward compensation to attain equal power consumption by a circuit. PAH logic generates equal amount of power by producing appropriate compensation transitions based on the input patterns. The logic consists of a functional part and a compensation part in which the former evaluates the logic operation, whereas the latter produces a requisite number of transitions to ensure constant HW of the output.

Bridge-boost logic (BBL) Lu et al. [139] recommended a dual-rail charge recovery logic, called BBL, that recovers charge from gate fanouts lowering energy dissipation. Such a gate consists of an evaluation and a boost stage where a bridge transistor is used in the boost stage to equalize currents in the evaluation stage to remove switching-dependent signatures from the power profile. Unlike other charge-recovery topologies [140], BBL gates endorse higher supply voltage than V_{th} to attain high operating speeds.

Machine-learning (ML)-based PAA relies on the relation between the most correlated key's hypothetical HD to the measured power. Shan et al. [141] introduced a machine-learning-based methodology to break this relationship. They proposed to compromise on the HD probabilities of intermediate data to make it unrelated to the correct sub-key. The HD redistribution mapping is based on an ML algorithm of dynamic programming. The compensation power is generated by altering the S-box inputs by a requisite number to produce the expected dynamic power.

Dual-rail flush logic (DRFL) Lu et al. [142] presented a static dual-rail CMOS logic called dual-rail flush logic, which recognizes gates in evaluation mode when inputs and outputs present valid complementary logic values. The gate is assumed to be in a precharge state when inputs are the same. The gate is toggled between the states ensuring only one output goes either high or low, depending upon the inputs. The energy consumption of each DRFL gate remains the same throughout its operation, irrespective of the input sequence.

Current domain signature attenuation (CDSA) Countermeasures employing noise injection[143], although reduce SNR, suffer from huge power overheads. The switched-capacitor current equalizer [124] also endures large passives, including onboard inductors, and has multiple trade-offs. In order to maintain a constant voltage across the crypto current, the ideal implementation of series LDO also leaks critical information inherently [95].

Das et al. [144] [145] proposed a countermeasure called CDSA, in which the current originating from the supply is stated to remain independent of the crypto-current. The current signature is suppressed before reaching the supply pin by embedding the crypto-core within a CDSA hardware. The MTD for PAA is enhanced by the square of the attenuation factor ($MTD \propto AT^2$). Ghosh et al. [8] further improved the countermeasure by adopting signature attenuation in the current domain and is made fully synthesizable using digital current sources, a control loop and a bleed. It further combines an attenuation circuit with a time-varying transfer function to boost the MTD.

Galvanic isolation technique Countermeasures with voltage regulator and power management techniques, such as switched capacitor current equalizers, analog, and digital low dropout regulators, and buck converters [7] [82] [123] [131] isolate external supply pin (V_{CC}) or randomize the signatures of the supply current. However, the shared external ground pin (V_{SS}) between crypto-core and power converter still remains vulnerable to SCA attacks. This issue is further aggravated in modern SoCs wherein multiple V_{SS} pins are arranged within a ball grid array (BGA). Side-channel information can be monitored by tracking the voltage bounce and substrate noise coupling [146] on these V_{SS} BGA pins.

To neutralize these effects, Wang et al. [147] introduced a galvanically isolated (GI) power delivery mechanism that isolates the AES core from external V_{CC}/V_{SS} pins. These pins are completely isolated from the external supply and ground pins by using a deep n-well technology and an integrated charge-pump-based power delivery. The proposed approach is based on the galvanic isolation principle employed in high-voltage power converters[148]. Based on the principle of transformers, circuits on the secondary side of the high-voltage power converter are galvanically isolated from high-transient voltages and currents on the primary side. The AES core achieves isolation by using a reconfigurable capacitor bank with back-end MoM (Metal-over-Metal) capacitors. The required charge for AES computation is supplied by the capacitor bank along with an integrated power management unit (PMU), thus, achieving complete isolation of the current loop from the external supply loop.

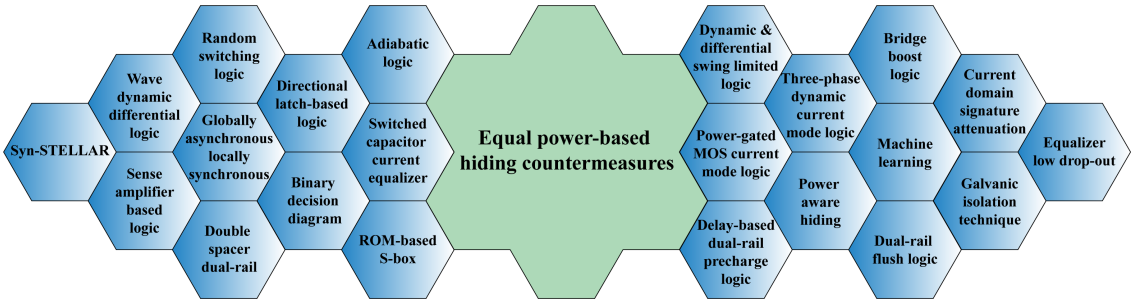


Figure 2.4: Equal power-based hiding countermeasures

Equalizer low-dropout (EQZ-LDO) Tokunaga et al. [123] flattened the supply current using a switched-capacitor current equalizer. However, the equalizer remains active during the entire encryption process costing 2.66× energy and 2× delay leading to large energy delay product (EDP) overhead of 5.32×. Since the attack rate is typically low during the lifespan of a device, such an active-for-all-rounds design wastes a lot of energy when it is not under attack. Shunt linear regulators [144] [95] and integrated regulators with control loop randomizers [149] [82], also waste energy and performance. Miura et al. [150] proposed an active-for-some-rounds equalizer active only during the first and last rounds of encryption which are the target instances. However, this technique leaves other rounds unprotected.

Kim et al. [151] proposed a novel detection-driven methodology where the device is made capable of detecting an attack attempt. The protection mechanism is embedded in the device, which is activated only when the attack is detected. An adversary typically probes the voltage drop across a non-negligible resistance (R_{nn}). An EQZ-LDO draws an extra current for a predefined amount of time and senses the IR-drop across R_{nn}. Upon detection of the attack, a protect command is sent to activate an embedded equalizer to restore the extra current ensuring constant current drawn.

SYNthesis-friendly Signature aTtenuation Embedded crypto with Low-Level metAl Routing (Syn-STELLAR) The analog nature of cascode CS slices, PMOS bleed path and voltage digital-to-analog converters (DACs) in the CDSA technique require manual re-design to scale across various technology nodes [144] [145]. Syn-STELLAR [152] takes care of this constraint by making a digital-friendly signature attenuation circuit employing digital current sources to attenuate the critical signature to attain higher security than its analog counterpart. The bleed path to bypass side-channel leakage is paved by Ring Oscillator (RO) which also acts as local negative feedback. Also, the time varying transfer function (TVTF) replaces the DC bias in the current-domain equalizer to convert it to digital and utilizes switch cap-based circuit for time-domain confusion to accomplish strengthened security.

The digital friendly signature attenuation technique is further utilized by Ghosh et al. [153] along with an intelligent attack detector circuit to detect PAAs and adapt to it to ensure the effectiveness of the countermeasure.

Hence, using the aforementioned countermeasures, a cryptographic device ensures an equal amount of power consumption every clock cycle. These strategies reduce the signal itself in order to lower SNR for an adversary. All the investigated designs under the category of equal power-based hiding countermeasures are collectively represented in figure 2.4.

2.2.2 Masking-based countermeasures

Masking approaches counteract PAAs by randomizing intermediate results of the executed cryptographic algorithm. This ensures the cryptographic device has a power profile independent of the intermediate values being processed in the algorithm. The striking feature of this approach is that an algorithm-level implementation of the countermeasure does not change the power profile of the cryptographic device. The masking countermeasures can be applied both at the algorithmic and circuit level. Some countermeasures associated with this category are enumerated below.

Boolean & arithmetic masking Messerges et al. [154] were the first ones to adopt the masking technique and proposed Boolean and arithmetic masking to mask all intermediate values of an encryption operation. Bitwise XOR operations are used as the mask operator in Boolean masking, whereas the mask operator in arithmetic masking uses addition and subtraction modulo 2^{32}. The randomized computation of a function f is represented by $f(u')$ where $u' = u \oplus r$ and r is an arbitrarily selected mask. If the function happens to be linear, the desired value $f(u)$ can be recovered from $f(u') = f(u) \oplus f(r)$. For a word employing a random mask, r_x, the masked values, x', are given as:

$$Boolean\ mask: \ x' = x \oplus r_x \tag{2.2}$$

$$Arithmetic\ mask: x' = (x - r_x)\ mod\ 232 \tag{2.3}$$

Adaptive/transformed masking Previous masking methods necessitated a masking condition in each AES step. Akkar et al. [155] proposed a technique which requires masking only at the beginning of algorithm. In the proposed transformed masking method, an additive mask is initially replaced by a multiplicative mask in a series of multiply and add operations, followed by a normal inversion, and finally, the multiplicative mask is transformed into an additive mask again. The value of the mask at any step needs to be known to re-calculate the expected value after completion of the algorithm. Its first hardware implementation was performed by Meyer et al. [156].

Embedded multiplicative masking Golić et al. [157] pointed out that a multiplicative mask fails to prevent a DPA attack as it does not blind a zero. It is known as the "zero-value problem", where a straightforward masking leads to a potential security vulnerability. The multiplicative mask is used to mask only non-zero values; hence, an attacker obtains information on $A_{i,j}$ if the values before (i.e., $A_{i,j} \oplus X_{i,j}$) and after (i.e., $(A_{i,j} \oplus X_{i,j})$ - 1) operations are detected.

In [155], the adaptive masking technique utilizes the multiplication in $GF(2^8)$ and integrates the conventional binary additive masking with the multiplicative masking of data. This multiplicative masking technique is vulnerable primarily because of the zero-value problem towards the S-box inputs and the removal of binary additive mask in order to apply the multiplicative mask. In order to solve this problem, Golić et al. [157] proposed the embedding of $GF(2^8)$ into a larger algebraic structure in a random manner.

Full hardware implementation of AES computations on masked data In the GF inverse calculation in SubBytes operation, binary AND operations need to be performed for multiplication and inversion in $GF(2^4)$. The actual (unmasked) bits may be revealed if the AND computations are performed on masked data and its corresponding mask correction.

Trichina et al. [158] proposed a new method of calculating inversion in the field $GF(2^8)$ by reducing it to inversion in the composite field $GF(2^4)$. The following relation holds for x_i and y_j masking the "real" bits, a_i and b_j -

$$(a_i \oplus x_i).(b_j \oplus y_j) = (a_i.b_j) \oplus (a_i.y_i) \oplus (x_i.b_j) \oplus (x_i.y_j) \tag{2.4}$$

Basically, the problem of inversion of masked data can be effectively reduced to the problem of computing a binary AND operation on masked bits of the data and corresponding mask correction without revealing the actual data bits.

Provably secure masking of AES The adaptive masking method [157] rather than randomizing all intermediate results puts up an experimental argument that using the method, the HWs of all intermediate results are distributed in roughly the same way, independent of the plaintext and the secret key. Blomer et al. [159] proposed a provably secure masking method with an assumption that an adversary is capable of acquiring an intermediate result. The method involves calculation of inverse using an optimal addition chain or square-and-multiply algorithm. Inputs being additively masked values, the square-and-multiply algorithm corrects the result of every single operation in order to obtain the desired result.

S-box inversion in GF(2^2) All the AES operations are linear, which can be masked in a straightforward manner, except the nonlinear operation involved in finite field inversion in the S-box SubBytes operation. Oswald et al. [160] proposed a combination of additive and multiplicative masking based on composite field arithmetic to mitigate the zero value problems highlighted in [155] [158]. The proposed method employs S-box inversion operation in $GF(2^2)$ field since the operations in this field are linear and can be easily masked.

Masked dual-rail precharge logic Conventional masked logic styles [161] [114] suffer from glitches, which are small spikes at gate outputs, due to unbalanced gated delays. Mangard et al. [161] analysed the side-channel resilience of masked circuits due to glitches, whereas Suzuki et al. [114] reported the glitch-modeling technique to evaluate attack resistance. Mangard et al. [162], in another set of work deduced the circuits' susceptibility to DPA attacks, and Suzuki et al. [163], also in another set of work, revealed that random masking by combinational circuits leak information due to glitches. A close analysis of masked multipliers [160], [159] showed that XOR gates employed in multipliers accounted for leakage in the side-channel. Although RSL claims to avoid glitches, the new standard cell library needs careful timing of enable signals.

Noting these developments, Popp et al. [164] proposed the usage of majority gate as a countermeasure. The gate is available in a typical CMOS library, enabling semi-custom design flow without place-and-route constraints. MDPL employs the DRP logic by combining WDDL and RSL to prevent glitches. For each signal d_m, its complementary signal, $\bar{d_m}$, is masked using the same mask, m. The majority function, MAJ, takes six dual-rail inputs $(a_m, \bar{a_m}, b_m, \bar{b_m}, m, \bar{m})$ and produces two outputs $(q_m, \bar{q_m})$.

Threshold implementation Non-linear S-box operations being the fundamental reason for side-channel leakages, conventional masking techniques call for new random values after every non-linear operation. Nikova et al. [165] proposed the threshold implementation method for masking, which constructs secure linear circuits for non-linear transformations

utilizing secret sharing [166] [167], threshold cryptography [168], and multi-party computation protocols. Bilgin et al. [169] explored the necessity of re-masking and proved that re-masking only a fraction of the shares under certain conditions is sufficient. For a masked AND gate realizing $z = x\ AND\ y$, the characteristics of the circuits implementing one of the functions, f_i, are independent of x, y and z, if the input shares follow the secret sharing. Consequently, the mean power consumption of each individual circuit is independent of x, y and z, even in the presence of glitches.

In another set of TI-based work [170], the AES S-box replaced expensive D flip-flops with low-cost synchronization circuits, such as, customized tri-state XOR gates, tri-state buffers, and D latches, efficiently coupled with Critical Path Replica (CPR) circuits.

Improved MDPL (iMDPL) Early propagation effect (EPE) was identified as a potential side-channel leakage in logic styles, such as, SABL [110], WDDL [111] and MDPL [164]. DRSL [171], although attempted to solve the EPE, could not completely avoid it in the precharge phase.

Popp et al. [172] indicated that differential encoding of the signals in their MDPL circuits proposed earlier allow detection of the time instant in evaluation phase when all the input signals of a cell are in a valid differential state. The instant of evaluation in a cell must be delayed until this point in time to avoid EPE. Hence, they proposed an advanced version of MDPL, known as iMDPL in which the evaluation-precharge detection unit (EPDU) ensures evaluation of logic only after all the input signals have arrived differentially.

Moradi et al. [173] revealed that logic masking in MDPL and iMDPL involving more than a flip-flop to share single-bit masking does not succeed in preventing information leakage. Also, the same research group exhibited in another study [174] that imbalances caused during routing between complementary mask trees on a chip exhibit possible leakage in iMDPL.

Pre-computation tables method Kim et al. [175] proposed to mask AES with higher orders which involves the calculation of inversion over composite fields [21] [22]. Sub-field operations, such as multiplication, square, scalar multiplication and isomorphism over $GF(2^4)$ are pre-computed and stored in tables. The masking operations are then performed for XOR, $GF(2^4)$ multiplication, and $GF(2^4)$ inversion.

Shamir's secret sharing scheme Goubin et al. [176] proposed a masking scheme as a substitute for Boolean masking. It relies on Shamir's secret sharing [167] and is processed using multi-party computation methods [177]. In this scheme, the 8-bit implementation output, z $\in GF(256)$ is manipulated under the form $(x_i,\ P(x_i))_{i=0,d}$ where $x_i \in GF(256)$ is a polynomial of degree d such that $P(0) = Z$.

Rotating S-box masking (RSM) Some masked S-boxes [178] [179] based on global LUT scheme [180] leak information as they are addressed by the mask data and mask. Nassar et al. [181] proposed an RSM scheme adhering to the re-computation method [180], addressed only by the masked data.

LUT-based masked S-box Wang et al. [182] considered an LUT-based masked S-box with all the masking operations carried out over $GF(2^4)$. Thus, masked AES operations require the plaintext and the masked values to be mapped from $GF(2^8)$ to $GF(2^4)$ and vice versa at the beginning and end of the operation, respectively.

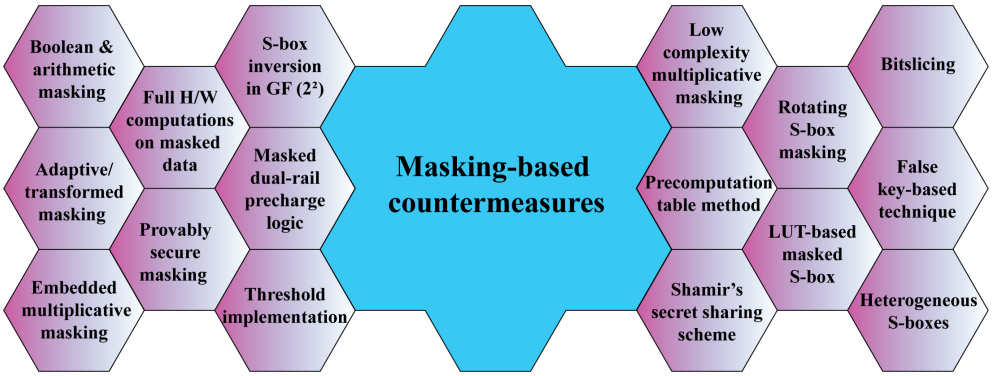


Figure 2.5: Masking-based countermeasures

Bitslicing Balasch et al. [183] proposed the bitslicing technique, which enables the implementation of a cryptographic algorithm by performing Boolean operations sequentially. Bitwise instructions, thereby allowing masking at the level of Boolean gates.

False-key-based technique Yu et al. [184] proposed a false key-based technique in which the round keys of the algorithm are associated with constant intermediate data to generate false round keys. It differs from the conventional masked AES technique based on the stage in the encryption process where masking operation is performed.

Heterogeneous S-boxes Kumar et al. [185] [186] proposed a lightweight secure AES with three strategies: heterogeneous S-boxes, linear masking of MixColumns, and key addition with dual-rail. The homogeneous S-boxes are replaced with a pair of heterogeneous ones using two distinct sets of GF-polynomials. Dual-rail XOR/XNOR gates are used to compute true and complementary outputs, resulting in data invariant switching activity. A non-linear digital LDO used along with these arithmetic countermeasures boosts security [86].

Low complexity multiplicative masking scheme Zhou et al. [106] proposes a low complexity multiplicative scheme for AES designs employing only one S-box, targeting resource-constraint applications. With constant multipliers having much lower complexity than the expensive general multipliers, the former kind are employed with two random non-identical field elements. A random bit is utilized to make a decision about which of the two multiplications results ought to be used as the finite field inverter input, in each clock cycle. In another multiplicative masking scheme, the additive masked inputs were converted to multiplicative domain before the S-box operations [187].

Thus, employing these countermeasures, intermediate values of the cryptographic algorithm are concealed using masks generated during processing of the algorithm. The masks help in invalidating the link between the predicted hypothetical emission/power consumption values (bound to the selected intermediate operation) and the actual values processed by the cryptographic primitive. Consequently, the power consumption of operations on randomized data is not correlated with the actual plain intermediate data. All the investigated countermeasures under the category of masking are collectively represented in figure 2.5.

Finally, the discussed countermeasures across the aforementioned categories are summarized in Table 2.2 highlighting the consumed overheads surmounting their respective unprotected designs. Also, the offered security by these countermeasures is mentioned providing an idea of the overheads which need to be traded off with security.

Table 2.2: Hardware resources and security metrics of various countermeasures

Countermeasure	Process	Standalone AES power/frequency	Design overheads			MTD	Remarks
			Area	Power	Performance		
Adaptive/transformed multiplicative masking [155]	90 nm	-	185.42%	-	159.6%	-	Masking only at the beginning of algorithm.
Adaptive/transformed multiplicative masking [155]	250 nm	-	-	-	-	1M	"same as above"
S-box inversion in GF(2^2) [160]	250 nm	-	-	-	-	1M	S-box finite field inversion in GF(2^2).
Wave dynamic differential logic (WDDL)[188]	180 nm	200 mW @50 MHz, 1.8 V	210%	270%	74.2%	1.2M	Successive stages of the circuit are precharged one after another.
Switched capacitor current equalizer [124]	130 nm	44.34 mW @110 MHz, 1.2 V	7.2%	33%	50%	>10M	Uses capacitors for isolation between encryption core and power supply
Random delay generation [67]	Atmel AVR μC	-	0%	0%	862 cycles	45K	Software methodology utilizing the time dimension.
Pseudo-RSL (Random switching logic) [115]	130 nm	24 MHz	-	-	43%	1M	Standard-cell design of Random Switching Logic.
Ring oscillator (LUT-based) [69]	90 nm	-	19%	-	0%	1M	Mounted on the S-box; no extra critical path delay.
Ring oscillator (CFA-based) [69]	90 nm	-	53.13%	-	0%	1M	"same as above"
Improved random delay generation [68]	Atmega 16 AVR μC	-	0%	0%	953 cycles	>150K	Enhances granularity of random delay generation.
Algorithmic balancing [131]	130 nm	@50 MHz	104%	-	0%	1M	Uses complementary logic gates (XNOR for XOR).
Threshold implementation [189]	180 nm	24.12 μW @100 kHz, 1.8 V	350%	262%	18%	-	No requirement of fresh random values after every non-linear transformation.
Threshold implementation [189]	SASEBO	-	-	-	-	100M	"same as above"
Ring oscillator [70]	90 nm	7.10 mW @200 MHz, 1 V	6.2%	18.5%	0%	>10M	Solves the 'reset' problem faced by ring-oscillator-based countermeasures.

2.2: Countermeasure attempts to secure AES designs

Countermeasure	Process	Standalone AES power/frequency	Design overheads			MTD	Remarks
			Area	Power	Performance		
Rotating S-box masking [181]	Altera Stratix-II	-	28% ALUT, 20% ROM	-	34%	200k	S-boxes addressed based on masked data and mask.
Supply current equalizer[150]	180 nm	10.9 mW @24 MHz, 1.8V	39.58% (without I/O)	23%	-	800k	Covers only the targeted first and last rounds of AES encryption.
Bridge boost logic (BBL) [139]	65 nm	98 mW @1.32 GHz, 0.41 V	200%	-29%	0%	940K	Employs bridge transistor to equalize currents.
Reconfigurable cryptoprocessor [90]	180 nm	33 mW @20 MHz	∼0%	5.77%	10.6%	1M	Executes instructions out of order and inserts random dummy operations.
Integrated buck regulator [7]	130 nm	10.5 mW @40 MHz, 0.45-1.05 V	2135 μm^2	5%	3.33%	>100K	AES and IVR clock desynchronized to forbid traces alignment.
ML-based Hamming Distance (HD) redistribution [141]	SAKURA-G FPGA	-	1% FF, 69% LUT	31%	0%	100k	Power compensation using neural programming.
ML-based Hamming Distance (HD) redistribution [141]	28 nm	0.18 mW @25 MHz, 0.42 V	36%	38%	0%	>1.5M	"same as above"
ML-based Hamming Distance (HD) redistribution [141]	28 nm	29.8 mW @870 MHz, 1.1 V	-	39.9%	0%	>1.5M	"same as above"
Random fast voltage dithering [78]	130 nm	13.1 mW @49.7 MHz, 0.89 V	6.6%	-3.5%	17.4%	1M	Randomly shifted clock edges, amidst global and local supply noise.
False key-based technique [184]	130 nm	@196.4 MHz	2.61%	0.24%	1.81%	>30M	Incorrect keys added in each encryption round.
Power aware hiding [138]	180 nm	4.47 units @50 MHz, 1.8V	2.21 mm^2	-	-	13.4M	Produces compensated transitions to maintain constant HW output.
Dual-rail flush logic [142]	65 nm	0.08 mW @10 MHz, 0.4 V	50%	42.86%	50%	>2M	Switching between precharge and evaluation modes.
Dual-rail flush logic [142]	65 nm	19.5 mW @430 MHz, 1 V	50%	65.25%	50%	>2M	"same as above"
Secure double rate registers[94]	65 nm	@20 MHz	33%	180%	0%	>100K	Protection of both combinational and sequential datapaths.
Secure double rate registers[94]	SPARTAN-6 FPGA	@20 MHz	28% LUT, 54% FF	190%	0%	>100K	"same as above"
Attenuated signature noise injection [95]	130 nm	@40 MHz, 1.2 V	60%	68%	0%	>1M	Suppresses the secret AES signature on supply pin.

Countermeasure	Process	Standalone AES power/frequency	Design overheads			MTD	Remarks
			Area	Power	Performance		
Digital LDO regulator with SNI & V-REF [83]	130 nm	10.9 mW @80 MHz, 0.84 V	36.9%	32%	10.4%	10M	Control-loop induced perturbations in a DLDO.
Microarchitectural randomization [97]	16 nm FinFET	391 μW @300 MHz	-	-	-	9,746	Randomizing the order of sub-round operations.
Heterogeneous S-boxes [186]	14 nm	11 mW @708 MHz, 750 mV	28%	23%	0.7%	12M	Protects the vulnerable attack points of AES.
Randomization techniques [101]	65 nm	336 mW @800 MHz, 1.2 V	2.3%	3.5%	4%	2M	Randomness in both time and amplitude dimensions.
Non-Linear-DLDO, arithmetic countermeasures [86]	14 nm	-	10%	8%	0.7%	1B	Loop randomizations to improve frequency-domain attack resistance.
Edge-chasing quantizer (ECQ)-based digital low dropout regulator [149]	65 nm	3.85 mW @40 MHz, 1.1 V	27.5%	19.4%	4.54%	>7M	Input voltage difference quantization performed using ring oscillators.
Current-domain signature attenuation [145]	65 nm	0.8 mW @50 MHz, 0.8 V	36.7%	49.8%	0%	>1B	Signature suppression of crypto-current in the current domain.
Digital signature attenuation and time-varying transfer function [8]	65 nm	189 μW @ 10 MHz, 0.8 V	28%	33%	0%	>1.25B	Obfuscations in time-domain using a switched capacitor circuit.
Galvanic isolation [147]	40 nm	23 mW @40 MHz	42.5%	130%	20%	>3M	Nullifies attack vulnerability due to supply and ground bounce
Equalizer LDO [151]	65 nm	0.0354 mW @3.3 MHz, 0.45 V	51.85%	1.84%	-	>10M	Protection activated only when device under attack.
Syn-STELLAR [151]	65 nm	0.15 mW @10 MHz, 0.8 V	52%	50%	0%	>1.25B	Analog-based signature attenuation utilized with digital current sources, scalable over technology nodes.
Low complexity multiplicative masking scheme [151]	Intel 4	@545 MHz, 0.75 V	65%	-	4%	>850M	Additive masked inputs converted to multiplicative domain before the S-box operations.

CHAPTER

3

S-BOX HARDWARE ANALYSIS TO IMPROVE AES' INTRINSIC SECURITY

Contents

3.1 S-boxes under investigation 50
3.1.1 Canright S-box 51
3.1.2 CMT S-box 51
3.1.3 Maximov S-box 51
3.1.4 Masoleh S-box 52
3.2 Evaluating the investigated S-boxes 52
3.2.1 Hardware resources analysis of the S-boxes 52
3.2.2 Hardware complexity/Linearity analysis of the S-boxes 53
3.2.3 Hardware security analysis of the S-boxes 53
3.3 Chapter summary 57

An efficient AES design needs to meet the resource constraints for an IoT edge device, in addition to providing a high resilience from attackers. The most important aspect of designing AES is the SubBytes round function which comprises of 16 S-boxes. The essence of this function stems from the fact that it is the only nonlinear function in the algorithm meant to provide severe confusion to the processed plaintexts. Although the task of each S-box is to substitute a pre-computed value, it is very taxing in terms of area and power when done using Look-Up Tables (LUTs) which are very humongous in size owing to the address-decoding logic circuitry required for correct mapping of inputs and outputs. Also, the significance of SubBytes round function in AES can be understood from the fact that it consumes 75% of the total AES power consumption owing to which it serves as the attack point for adversaries. The CPA attack model is based on the S-box operations involved in the SubBytes operation, thus enforcing Sbox design to demand dire attention. The literature portrays numerous S-boxes spanning various design targets like area minimization, power curtailment, performance boosting, etc. However, an obvious question for an AES designer is, "Which S-box should I choose?" Although designers enjoy the liberty of choosing S-boxes based on their design targets, there lies an unanswered question about them, "Are they going to make any difference in terms of their security offerings?"

This chapter undertakes an effort to answer this question by evaluating some famous and recent S-boxes from the literature. The Look Up Table (LUT)-based S-box is made to serve as a reference and some Composite Field Arithmetic (CFA)-based S-boxes analysed in terms of their hardware resources and security provided. The significance of the undertaken work can also be appreciated based on the fact that 16 copies of an S-box are utilized in a single SubBytes function and 4 copies in the key scheduling operation in an AES' round operation. Hence, the S-box can be expected undergoing a total employment of 200 times considering all the 10 round operations, justifying the significance of this thesis chapter. This work performs a novel effort and investigation of boosting the 'intrinsic' security of an unprotected AES by studying the security offered by various S-boxes and choosing the best one.

3.1 S-boxes under investigation

Owing to its simplicity in design technique, an LUT-based S-box is the first and foremost choice of S-box for an AES designer. For a hardware AES implementation, usage of LUT-based S-box will require storing 256 bytes, apart from the address decoding and fetching circuitry. To facilitate parallel processing of 16 bytes of AES data, 16 such copies of the LUT-based S-box would be required for the SubBytes round operation. Such an intensive requirement of hardware resources clearly rules out its usage for applications, such as, IoT where area and power play a pivotal role. The address decoding and fetching circuitry forming the core logic of such a design renders it unadvisable for usage due to the immense area occupancy [24] [36]. Literature rerouted towards LUT-less logic gates-based S-box design [23] [25] [190] as its solution using Galois Field (GF) theory [191]. The design target has always been to minimize the size of the S-box by reducing its gate count. The S-boxes shortlisted for this work are the smallest ones in terms of gate count, highlighted in the literature. This work chooses four low gate count S-box designs, namely CMT [28], Canright [26], Maximov [33] and Masoleh [192], for the investigation. CMT and Maximov S-boxes have been developed using linear transformation of input and output signals, Canright S-box is built on $GF(((2^2)^2)^2)$ and Masoleh S-box on $GF((2^4)^2)$ normal basis. With 16 S-boxes employed for the SubBytes operation in an AES design, a wise choice of S-box is expected to provide fruitful results in terms of hardware resources savings. Most importantly, this work

intends to perform a first-time study of the security provided by these S-boxes owing to their logic gates-based construction.

3.1.1 Canright S-box

The S-box function of an input byte is performed by calculating its multiplicative inverse followed by its affine transformation. The multiplicative inverse is carried out in Galois Field, $GF(2^8)$ and the affine transformation involves a matrix multiplication of the inverse with predefined matrices. For a byte, direct calculation of the inverse would be a very costly affair as the operations would involve a 7^{th} degree operation. Hence, Canright used the finite field property of isomorphism to transform the operations from a higher field, $GF(2^8)$, to a 2-bit operable $GF(((2^2)^2)^2)$ field with $GF((2^4)^2)$ as the intermediate field.

An element of $GF(2^8)$ in normal basis can be represented over $GF(2^4)$ as:

$$r(y) = y^2 + \tau y + \nu = (y + Y)(y + Y^{16}) \tag{3.1}$$

where, $\tau = Tr_{F_{256}/F_{16}}(Y)$ is the trace, $\nu = N_{F_{256}/F_{16}}(Y)$ is the norm of Y. For representation of an element of $GF(2^4)$ over $GF(2^2)$, the normal basis $[Z^4, Z]$ can be used, whose trace is $T = Tr_{F_{16}/F_4}(Z)$ and the norm is $N = Tr_{F_{16}/F_4}(Z)$. An element of $GF(2^2)$ can be represented over $GF(2)$ using the normal basis $[W^2, W]$, whose trace is ω =1 and norm, $\psi = 1$.

3.1.2 CMT S-box

CMT represents a team working on the problem of finding "good" circuits over $GF(2)$ or if stated otherwise, circuits using AND, XOR and XNOR gates. Good circuits, here, imply small, low-depth and fewer AND gates. The designed circuits are defined over the basis $\{\oplus, \wedge, 1\}$ such that any Boolean circuit can be transformed into this form, with $\oplus$ denoting XOR gates, and $\wedge$ denoting AND gates. The circuit operations can be considered to be performing Boolean logic or arithmetic modulo 2. Circuit components connected using $\wedge$ gates are called nonlinear, whereas those free of them are called linear. The number of $\wedge$ gates denotes the multiplicative complexity of the circuit.

The foundational basis of this S-box design technique is that circuits with low multiplicative complexity tend to have large linear portions. Thus, a two-step process of reducing multiplicative complexity and then optimizing the linear components is followed enabling the circuits to be small. This S-box design involves a combinational logic optimization in which the non-linear gates of the circuit is reduced and then, the number of gates in the linear components in the already reduced circuit, is minimized.

3.1.3 Maximov S-box

This S-box design is constructed by finding the smallest circuit which realizes a given linear transformation on n input signals and m output signals, with a constraint of a maximum depth, $maxD$, of the circuit. Arrival of input signals to the circuit with variable delays, and output signals readied at different depths are some possible requirements of this scheme. For a binary matrix, M_{mXn}, with maximum allowed depth, the circuit of depth, $D \leq maxD$, is to be traced with the minimum number of 2-input XOR gates, such that it computes $Y = M.X$. It implies that for n bits of input $X = (x_0...x_{n-1})$, the circuit is expected to determine m linear combinations $Y = (y_0...y_{m-1})$. A circuit which is able to realize the given system of linear expressions is referred to as the 'solution'.

Table 3.1: Resources comparison of various S-boxes and their AES implementation on UMC 65 nm technology node

	S-box				AES			
	Area (μm^2)	**Power** (μW)	**Delay** (ns)	**GE**	**Area** (μm^2)	**Power** (μW)	**Delay** (ns)	**Throughput** (Gbps)
LUT	852.12	2.309	1.29	591.75	23,588.28	90.364	2.83	3.769
CMT	409.32	5.107	2.85	284.25	14,584.67	106.977	4.13	2.583
Canright	336.24	4.811	3.14	233.5	13,151.88	101.273	4.48	2.381
Maximov	325.8	4.265	2.40	226.25	12,914.28	97.824	3.68	2.899
Masoleh	315.36	4.295	2.37	219	12,705.48	98.4	3.64	2.930

3.1.4 Masoleh S-box

This is the smallest S-box available in literature which has been designed by using new tower field representation over normal bases, and optimizing each and every block inside it. With isomorphism allowing change of bases of the finite-field polynomials amongst the fields, $GF(2^8)$, $GF((2^4)^2)$, $GF(((2^2)^2)^2)$, all the possible mappings are searched to find the one occupying the minimum area. For each design, the input and output mapping of 16 variables, normal basis field representations in the tower field $GF(((2^2)^2)^2)$ are studied, with each mapping formulated by employing four different generators. Eventually, the inversion circuitry of the S-box over the tower field is developed, comprising of exponentiation, subfield inversion and output multiplier blocks to perform the total S-box functionality.

3.2 Evaluating the investigated S-boxes

LUT-based S-box, due to its ease in design, is the most commonly used S-box by AES designers. However, owing to its design definition, it occupies a humongous area making the AES design unfavourable for resource constraint IoT-devices. Designers tend to use the inefficient LUT-based S-box owing to the mathematical complexity involved in understanding the finite-field arithmetic involved in CFA-based S-box designs. Circuit designers have been in the quest of reducing the size of S-box by reducing the number of logic gates required to build it, but this work presents the impact of the internals of S-box on the security offered.

3.2.1 Hardware resources analysis of the S-boxes

A comparison of the aforementioned S-boxes is performed on a common platform of UMC 65nm technology node for a fair comparison using Synopsys Design Compiler. Table 3.1 depicts the area, power and delay for the S-boxes and their corresponding AES designs. In addition, gate equialent (GE) for the S-box designs and throughput for the AES designs are reported. Masoleh and Maximov S-boxes depict lesser area owing to reduced GEs, with similar effect on the AES designs employing them. With LUT-based S-box out of choice due to its humongous area occupancy, Masoleh and Maximov S-boxes consume lesser power than the other CFA-based S-boxes providing similar impact on their AES designs. With IoT

Table 3.2: Hardware resources comparison of various S-boxes and their AES implementation on UMC 65 nm technology node

S-box type	Hardware complexity	# Linear gates	# Nonlinear gates
CMT	77 XOR + 4 XNOR + 32 AND	81	32
Canright	74 XOR + 6 XNOR + 34 NAND + 6 NOR	80	40
Maximov	58 XOR + 6 XNOR + 27 NAND + 5 NOR + 6 MUX	64	38
Masoleh	55 XOR2 + 1 XNOR + 32 NAND + 6 NOR + 4 OAI + 6 NOT	56	48

applications requiring formidable throughput, the delay provided by the two AES designs allow an adequate throughput of ∼3 Gbps.

As mentioned in the previous chapter that hypothetical power consumption values involve calculation of HD between the hypothetical intermediate values, v_{ij}, and the data blocks involved in the encryption process, d_i, thus, the S-box with lesser GE would imply lesser gate-based transitions, thus implying lesser HDs. The choice of S-box also becomes very important from the perspective that it occupies 75% of the overall AES power [46]. Hence, out of the four CFA-based S-boxes, Maximov and Masoleh S-boxes seem to be the favourable candidates for AES designs in resource constraint IoT applications.

3.2.2 Hardware complexity/Linearity analysis of the S-boxes

Nonlinearity is an important parameter of a cipher involved in the cryptographic processes [193]. For its hardware design, nonlinearity has a direct relation with the type of logic gates which have been used for the design. Initial S-box designs merely cared about reduction in the logic gate count, however, recent S-box designs have started looking into reducing linear gates in S-box designs [33] [192]. S-box, being a nonlinear byte substitution step in AES, is expected to offer a very high degree of nonlinearity, however, the usage of linear gates tends to weaken the nonlinear effect. Table 3.2 presents a novel analysis of the contributions made by linear and nonlinear logic gates for the selected CFA-based S-box designs. The table indicates Masoleh S-box to be designed with the least number of linear gates in comparison to the designs involving other S-boxes.

The linear and nonlinear gate count mentioned in Table 3.2 is presented as pie-charts in Figure 3.1 indicating the share of linear gates out of the total gates used for design of the S-box. Circuit components connected using xor gates are termed linear, whereas those free from xor gates are termed nonlinear. Masoleh S-box seems to be having the least share of linear gates, as portrayed by the pie-charts. Reduction in its linear gate count would lead to lesser switching between the gate outputs. With such gates forming the foundational basis of the CPA attack model (as mentioned in equation 1.5, Chapter 1), their minimized switching would contribute insignificantly to their Hamming Distance, thereby weakening the basis of CPA attacks. Hence, Masoleh S-box is expected to display the highest security among other S-boxes by virtue of its lesser linear gate count.

3.2.3 Hardware security analysis of the S-boxes

Having examined the resources consumption and complexity of the S-boxes, it sets up a very good platform to analyze their security. It is to be noted that higher security directly relates to the failure of the attack model. For that to happen, the correlation between the hypothetically generated power values and the real power values needs to be weakened

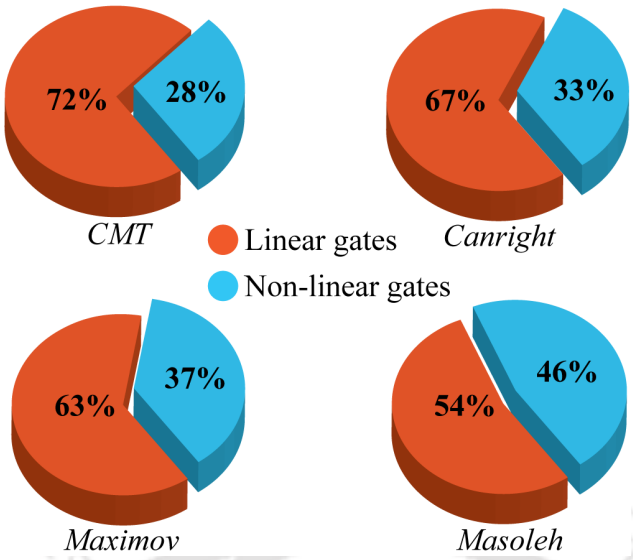
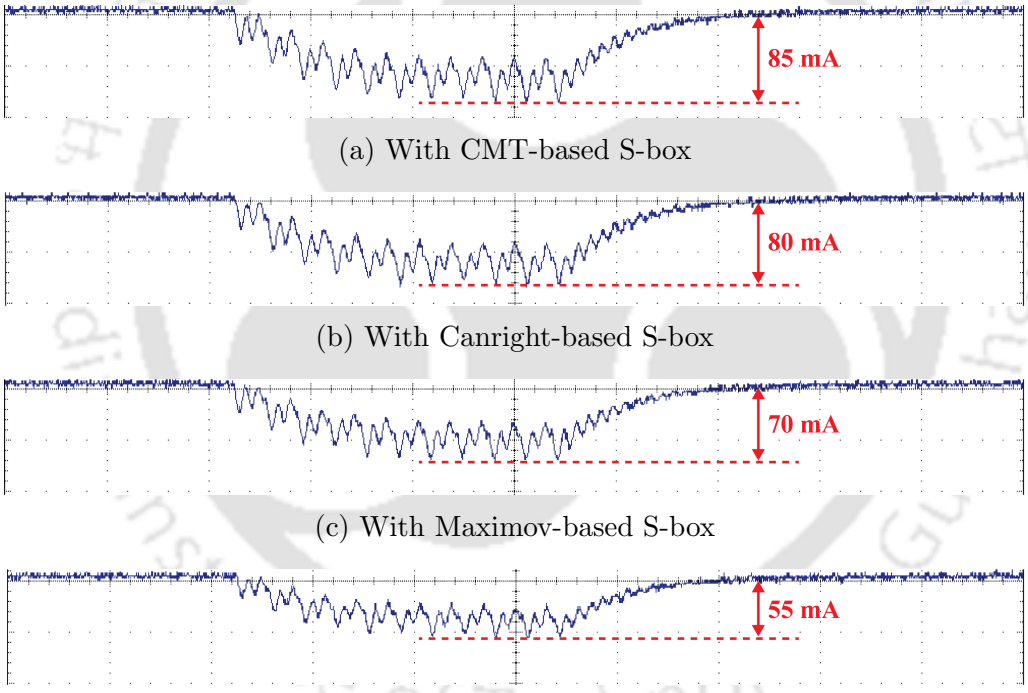


Figure 3.1: Share of linear and nonlinear gates for the S-boxes



(a) With CMT-based S-box

(b) With Canright-based S-box

(c) With Maximov-based S-box

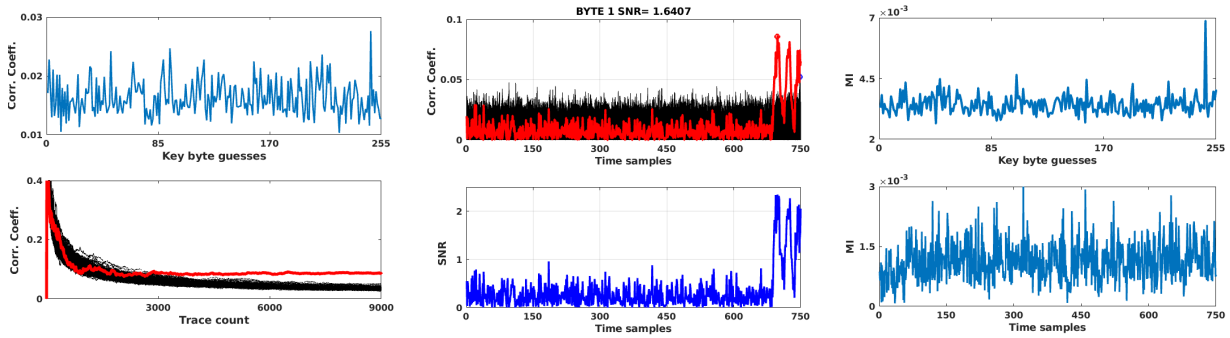
(d) With Masoleh-based S-box

Figure 3.2: AES power trace comparison for different S-boxes

or broken. The compared values basically correspond to the same set of plaintexts. Hence, reduction in S-box switching is bound to convey lesser HD-related information of the internal processing at the AES' last round which serves as the attack point.

Trace pattern comparison

In order to examine the effects of gate-based switching of the S-boxes, the power traces of AES designs with the S-boxes under investigation are generated on SASEBO by passing



(a) MTD plot (b) SNR plot (c) MI plot

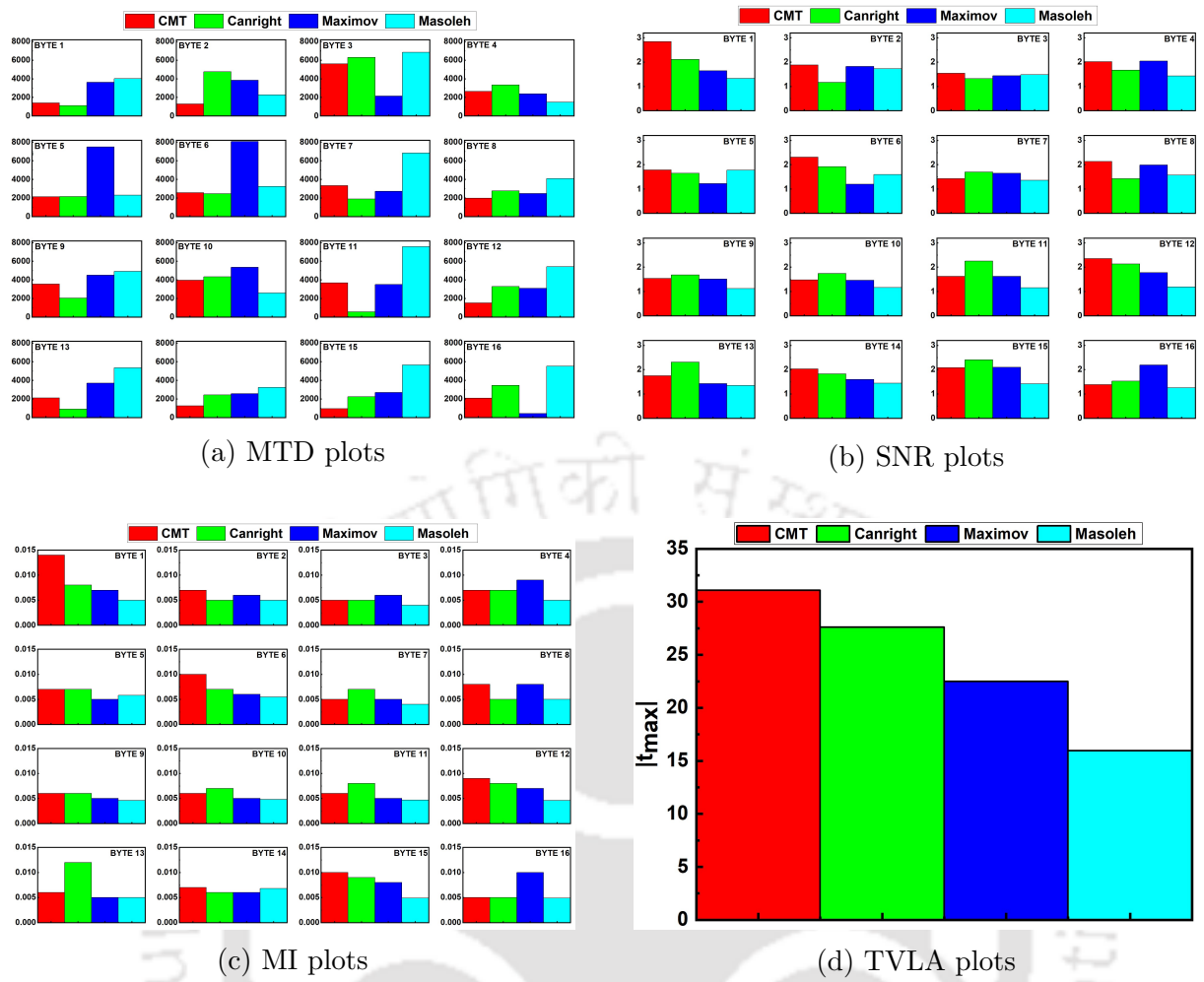
Figure 3.3: Attack results of sample byte 1 for Maximov S-box-based AES design

several plaintexts. The obtained trace patterns are, as displayed in Figure 3.2. The trace on the oscilloscope basically denotes the pattern in which the AES design running on SASEBO draws power (current) from the power supply. The power pin of SASEBO is tapped for the power side-channel information which is relayed to the oscilloscope using an SMA-BNC cable. Each trace distinctively depicts ten peaks corresponding to the ten round operations involved in AES. With the SubBytes round operation contributing to the major share of the AES total power consumption, it is an obvious conclusion that its contribution in forming the depicted trace patterns is also the most significant among other round operations. From the visible trace patterns, it is quite evident that Masoleh S-box with the least number of GEs has the least transitional switching magnitude followed by the lesser GE Maximov S-box. This can be directly correlated to their minimal GE values. This provides a clear indication that the Masoleh and Maximov S-box-based AES designs should reflect lesser HDrelated information thereby weakening the CPA attack model. A proportionate relationship of the GE and the switching magnitude is also evidently visible, as an incremental pattern is followed by both the parameters for Masoleh, Maximov, Canright and CMT S-box. Also, a hike of 54.54% in switching magnitude of current is observed for the highest GE CMT S-box compared to the least GE Masoleh S-box.

Security metrics evaluation

The assertion that reduced gate switching of S-boxes weakens the CPA attack model, is verified by evaluating the hardware security metrics, MTD, SNR, MI and TVLA. Power traces are generated on SASEBO by passing 9,000 plaintexts through AES designs with the investigated S-boxes, adopting an AES design frequency of 16 MHz and a sampling frequency of 1 GSa/s. A key point to be noted here is that the endeavor is to determine the S-box providing higher security, and not develop a totally secure AES design. Hence, upon attacking the designs with the S-boxes under consideration, the cipher key is expected to be retrieved. Figure 3.3 depicts a sample security metrics plot of byte 1 for an AES design employing Maximov S-box.

In the MTD plot, the correlation coefficient versus byte guesses indicate a peak standing out w.r.t. key value (F6). This indicates the correct key byte to have been recovered. Similarly, the correlation coefficient versus trace count in the MTD plot depicts the dispersion of the red curve (corresponding to correct key byte) from the sea of wrong curves in black (corresponding to wrong key bytes). The SNR plot records the correlation coefficient values



(a) MTD plots

(b) SNR plots

(c) MI plots

(d) TVLA plots

Figure 3.4: Byte wise analysis of hardware security metrics for AES with different S-boxes

of the generated power traces and plots it w.r.t. time instants time instants of their sampling. The highest correlation value corresponding to the correct key (red) is found to be greater than that of the wrong key (blue), indicating successful key recovery. Also, the SNR versus time samples plot clearly depicts SNR values > 1 towards the last round samples. An SNR of > 1 is considered to be extremely leaky and conveying significant information to the attacker. Finally, the MI versus key byte guesses in the MI plot, similar to the MTD plot, indicates a distinct peak corresponding to the correct key byte. When plotted against the time instant of their sampling, MI values are slightly towards higher range indicating significant mutuality of information between the hypothetical and real power traces.

Having undergone the exercise of interpretation of the security metrics plots, the key recovery attacks are performed on all the AES designs with the considered S-boxes for all the bytes, 1 through 16. They are collectively represented for an easy comparison in the form of bar graphs, represented in Figure 3.4. The motive behind this illustration is to identify the easier or tougher cracking of the cipher key bytes by every AES design type. Additionally, TVLA is also performed on the investigated designs whose maximum t-value is considered for each design. It is to be noted that TVLA is not a byte-wise process, rather signifies the information leakage alone by virtue of the t-value. One out of the four S-box types is expected to depict supremacy over others in all the metrics examined.

Table 3.3: Comparison of Maximov and Masoleh S-box-employed-AES designs w.r.t. earlier unprotected AES designs

S-box type	***Maximov*** ♠	***Masoleh*** ♠	**[94], 2018**	**[138], 2017**	**Canright [183], 2015**	**[194], 2009**	**LUT [188], 2006**
MTD	*8,078*	*7,588*	72	<2,200	2,000	4,000	2,133
Area(μm^2)	*12,914.28*	*12,705.48*	41,617	38,637	-	3,50,000	-
Area(GE)	*8.968k*	*8.823k*	20k	-	-	-	199k

♠Thesis results

Figure 3.4 depicts the highest MTD values for 11 bytes (numbered 1, 3, 7, 8, 9, 11, 13, 14, 15 and 16) corresponding to Masoleh S-box, 3 bytes (numbered 5, 6 and 10) corresponding to Maximov and 2 bytes (numbered 2 and 3) for CMT S-box. This is in exact decreasing order of their GE, as reflected upon in Table 2.1. Since SNR enjoys an anti-proportional relationship between each other as they utilize correlation coefficient for evaluation, a similar result is obtained with 11 bytes (numbered 1, 4, 7, 9, 10, 11, 12, 13, 14, 15 and 16) having the least SNR for Masoleh S-box, Maximov S-box pertaining to the least SNR for 2 bytes (5 and 6), and Canright S-box for 3 bytes (2, 3 and 8). The MI bar graphs also depict 11 least values for Masoleh S-box (numbered 1, 3, 4, 6, 7, 9, 10, 11, 12, 13 and 15), 2 for Maximov (byte numbered 2 and 15), and 3 for Canright (byte numbered 2, 8 and 16). Finally, the TVLA analysis of the designs indicate the least value for Masoleh S-box followed by Maximov and Canright.

Hence, from the aforementioned observations, it is clearly evident that incorporating Masoleh S-box in an AES design results in the highest security compared to incorporating other S-boxes. Most number of bytes with the highest MTD, lowest SNR, lowest MI and lowest t-score in TVLA, in comparison to the other S-boxes, confirms the assertion. Hence, as predicted at the outset of the discussion, having less GE and linear gates does weaken the CPA attack model, resulting in higher security.

A comparison of MTD and area of AES designs employing the two most secured S-boxes from our analysis, Maximov and Masoleh S-boxes, is made with unprotected AES designs prior to the discovery of these S-boxes, as shown in Table 3.3. Some state-of-the-art unprotected AES designs [94], [138], [183], [194], [188] are referred for comparison with the AES designs developed using Maximov and Masoleh S-box. The MTD improvement ranges from 2× to over 100× whereas the reduction in area ranges from 3× to 27×, depicting clear gains in terms of security as well as hardware resources upon utilizing these S-boxes. Thus, we can see an amplification in the intrinsic security of AES without addition of any actual countermeasure in the form of circuits, merely by opting for a wise choice of S-box. Also, the hardware savings provide a room for the inclusion of actual countermeasure with minimal overheads.

3.3 Chapter summary

Literature depicts plethora of countermeasures some of which are based on random data processing [94], feedforward compensation [138], etc. with very large area and power overheads on the AES design. The presented work makes a novel attempt and investigation to boost the intrinsic resilience of AES towards CPA attacks without incorporating any countermeasure. The foundational basis of the attack model is to record HD-based transitions involving S-box operations during the encryption process. The investigation involves

a three-dimensional analysis of four smallest S-boxes available in literature in terms of their hardware resources, hardware complexity/linearity and hardware security. The examination reveals that S-boxes with low gate count/GE and linearity contribute to minimal switching thereby weakening the attack model. The smallest S-boxes available in literature, namely, Masoleh and Maximov, apart from providing desirable area and power occupancies in AES designs for IoT applications, depict favourable hardware security metrics in comparison to their counterparts. Finally, the security enhanced unprotected AES is expected to provide amplified resilience when employed with small-size countermeasures, for IoT devices.

CHAPTER

4

IMPROVEMENT OF AES' RESILIENCE WITH NOVEL CFB MODE

Contents

4.1 Proposed rolling architectures for AES modes 60
4.1.1 Hardware efficient architectures for various modes 61
4.1.2 Novel CFB-64 mode for improved security 62
4.2 Establishment of the proposed attack model 63
4.3 Novelty of the proposed architectures 64
4.4 Hardware security metrics evaluation 66
4.4.1 Security metrics' trends depicted by the investigated modes 66
4.4.2 Security metrics evaluation of the proposed CFB-64 mode 66
4.5 Chapter summary 68

To facilitate parallel processing of information, National Institute of Standards and Technology (NIST) defined five modes of operation for AES, namely, Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB), Output Feed Back (OFB) and Counter (CTR) [195]. They are implemented as a 128-bit mechanism with additional inputs, such as, Initialization Vector (IV) and counter, apart from the conventional plaintext, ciphertext and key [196]. ECB and CTR are classified as non-feedback modes, whereas CBC, CFB and OFB are classified as feedback modes, depending on the necessity of previous ciphertext in the current run [197]. Plethora of work in the literature depict non-feedback modes employed in high-throughput applications owing to their possibility of pipelining [38] [198]. They provide architectural advantages as it allows parallelism, whereas the feedback modes are advantageous from the security perspective, but limits the speed of the AES architecture due to the loop dependencies [197].

With the discovery of PAAs [15], and an AES designer having the freedom to choose any mode of operation, their security and resilience to these attacks become an important aspect. However, there exists a severe gap in the literature with regard to this. ECB is the simplest and the most commonly used mode, however, with a drawback that encrypting two identical plaintexts with the same key leads to two identical ciphertexts [199]. This provides hints to the attackers to employ attacks, such as, reordering of blocks [200]. Some works designed the feedback modes with a focus on the AES architecture alone, and not the security aspects [201] [202] [203]. Another work implemented AES in ECB, CBC and OFB modes, offering an MTD of 8,168 [188]. Counter mode AES has been broken at an MTD of 2^{13} (8,192) against a smart card implementation [204] and at 200 on SASEBO [169]. The most recent works relating to AES' modes include an attempt to secure all its modes using key updation strategy [205], the CBC mode used for lowest critical path delay [206], and a multicore processor utilizing CBC mode for authentication process and CTR mode for confidentiality had its MTD evaluated in which the the processor operations executing parallelly with the cryptographic operations acted as a countermeasure [207].

However, upon adding countermeasures, the area and power overhead skyrocket by leaps and bounds [94] [190]. This thesis chapter investigates AES' standard modes of operation and proposes a novel CFB-64 mode which is more secure than other modes and various unprotected designs. The novel CFB-64 design will "act as a countermeasure" for the unprotected designs with minimal overheads, and qualify for battery-driven IoT applications imposing strict area and power constraints. This is another endeavor of the thesis towards boosting the intrinsic resilience of an unprotected AES design. In addition, this chapter suggests modified architectures for the standard modes and proposes a new CPA attack model fit to attack the feedback modes, as the standard model does not deem fit.

4.1 Proposed rolling architectures for AES modes

Since the thesis aims at minimizing hardware resources, rolling architecture is preferable over other architectures like unrolled pipelining or partial pipelined architectures. Such an architecture utilizes the same hardware dedicated for round operations in iteration, leading to immense hardware savings. The standard architectures of various AES modes presented by NIST necessitates duplication of the AES blocks which is not a good idea for resource constraint IoT edge devices. This section discusses proposed architectures for the various AES modes and a novel architecture aiming improved security.

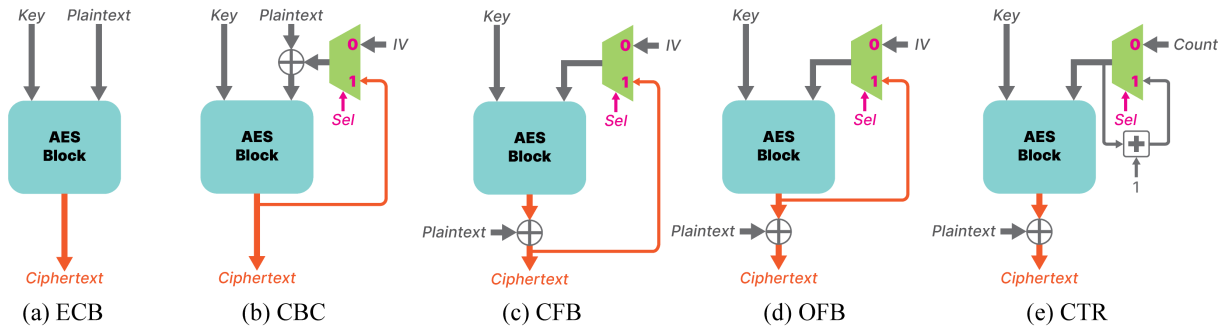


Figure 4.1: Proposed hardware-suitable rolling architectures for AES modes
($\oplus$ represents XOR operator)

4.1.1 Hardware efficient architectures for various modes

The standard modes' architectures defined by NIST hold multiple AES blocks in parallel with different peripheral implementations, such as, stage of involvement of plaintext in encryption and stage of tapping AES outputs to the next AES run [195]. These modes have been characterized to facilitate processing of enormous data at the software level. The multiple AES blocks employed in the modes render them unsuitable for hardware applications. With stringent area and power constraints on the AES to be used for IoT applications, architectures are proposed for these modes, which deem suitable for IoT hardware. Figure 4.1 depicts the proposals, where ECB mode is the simplest one producing ciphertexts from plaintexts in a straightforward manner using the key.

The CBC, CFB and OFB modes utilize an extra input, Initialization Vector (IV), in the first run of AES. In CBC, IV is replaced by the ciphertext second run onwards after being selected via a multiplexer (mux). In CFB and OFB modes, IV acts as the first virtual plaintext being fed to the AES block via the mux, and the real plaintexts are XORed with the AES block output. The only difference between these two modes is the point of tapping the second input of mux. CFB forwards the result obtained after the plaintext is XORed with the AES block output, whereas OFB passes the result obtained prior to the said operation. The CTR mode employs an additional input, counter, acting as a virtual plaintext throughout the AES processing, which gets incremented for every plaintext. Its final ciphertext processing resembles CFB and OFB modes.

The CFB mode has sub-types, such as, 64-bit, 8-bit and 1-bit versions. Only the 128-bit and 64-bit versions have been considered for this work utilizing the same proposed architecture, as other versions are expected to be very slow. A bit selection policy enables the XORing of s-bits of the output block with plaintext to form the ciphertext without considering the remaining (b-s) bits which do not form any portion of the output. These s-bits of ciphertext form the least significant bits of input block for which the (b-s) least significant bits of IV act as the most significant bits.

Table 4.1 presents the resource comparison of the AES modes, evaluated using UMC 65 nm technology node for ASIC platform and on the Spartan-3A XC313400DSP device for FPGA. The detailed discussion about the table is carried out after the discussion of the proposed mode architecture in the next sub-section.

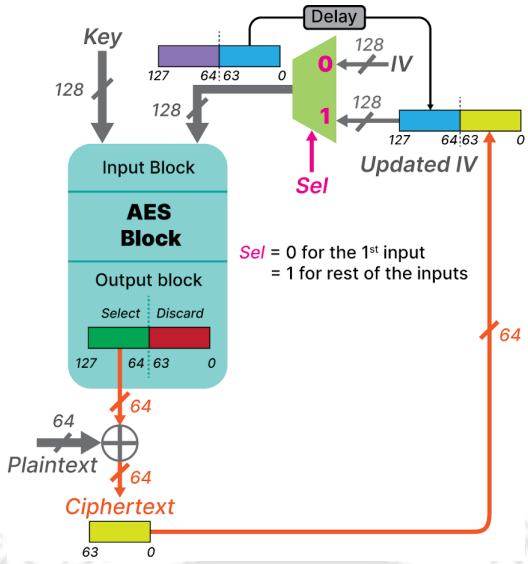


Figure 4.2: Proposed CFB-64 AES mode

4.1.2 Novel CFB-64 mode for improved security

Security, being the other aspect of our work apart from resources saving, a novel CFB-64 AES mode is proposed which is a modified version of 128-bit CFB mode. It is named so, because the generated ciphertext is of 64 bits. The construction of the proposed mode began with the keen observation of the existing CFB-128 mode. As evident from Figure 4.1(c), the existing CFB-128 mode passes IV as input in the first run and the 128-bit ciphertext of the previous run as input for the subsequent runs. Here, 128-bit plaintext is XORed with the output block to produce 128-bit ciphertext. An important observation in this case is that upon attacking the 1^{st} round of AES using Hamming Weight model, it becomes difficult to crack the cipher key, as the input depends on IV which is unknown to the attacker. But, it becomes easy to crack the key by attacking the 10^{th} round using Hamming Distance model, as the whole ciphertext is available to the attacker. Hence, the output block of the proposed CFB-64 mode in Figure 4.2 is restructured in such a way that the output is hidden from the attacker, thereby protecting the key. The input block structure is also slightly modified where the 128-bit input in the first run is IV, and for the subsequent runs, it is the concatenation of the least significant 64-bits of previous input and the previous 64-bit ciphertext. This makes input block more complicated due to the dependence on the ciphertexts of the previous two runs. After the AES processing of 128-bit input and 128-bit cipher key, the bit selection policy is employed on the output block, where only the most significant 64-bits of output are selected and XORed with the 64-bit plaintext to produce the ciphertext, and the remaining 64-bits of output are not considered which have crucial information about the cipher key.

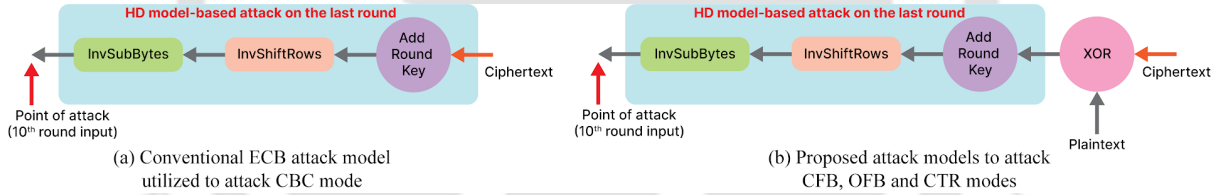
Table 4.1 presents the resource comparison of the AES modes, evaluated using UMC 65 nm technology node for ASIC platform whereas table 4.2 presents the comparison on the Spartan- 3A XC313400DSP device for FPGA. The ASIC results for the proposed CFB-64 mode indicate an area value lesser than all the modes except ECB, the least power value amongst other modes, and a formidable delay resulting in reduced throughput owing to only 64-bits produced as output. The FPGA results for the proposed CFB-64 mode imply a high LUT usage owing to the enormous combinational blocks in the design which results in a very less sequential FF occupancy. Similar to the ASIC results, power is the least among other investigated designs, with a compromise in throughput owing to the formation of 64-bit ciphertext output.

Table 4.1: Hardware resources comparison of various AES modes on ASIC

	ASIC			
	Area (μm^2)	**Power** (μW)	**Delay** (ns)	**Throughput** (Gbps)
ECB	12,705.48	98.41	3.63	2.938
CBC	16,185.6	86.43	3.79	2.814
CFB-128	16,841.88	112.98	4.18	2.552
OFB	15,725.88	84.79	3.69	2.8907
CTR	15,734.16	82.69	12.38	0.8616
Proposed CFB-64	15,178.68	78.73	3.67	1.453

Table 4.2: Hardware resources comparison of various AES modes on FPGA

	FPGA				
	LUT	**FF**	**Power** (mW)	**Delay** (ns)	**Throughput** (Gbps)
ECB	1,037	3,686	65	6.363	1.676
CBC	2,699	1,149	50	6.404	1.666
CFB-128	2,933	1,149	59	7.111	1.5
OFB	2,846	1,149	68	7.0	1.524
CTR	2,569	1,149	49	7.32	1.457
Proposed CFB-64	2,837	1,021	44	6.37	0.8375



(a) Conventional ECB attack model utilized to attack CBC mode

(b) Proposed attack models to attack CFB, OFB and CTR modes

Figure 4.3: Proposed attack models for assessing the AES modes

4.2 Establishment of the proposed attack model

The conventional CPA attack is performed on the ECB mode using MTD and SNR, based on the 'correlation coefficient' parameter. Similarly, Mutual Information Analysis (MIA) attack is performed using the 'entropy' parameter. These parameters are calculated using real power trace samples and their hypothetical values, using a Hamming Distance (HD) model. In all digital circuits, the primary share of the overall power consumption is caused by CMOS gate transitions which serve as the basis for the HD power consumption model. Eventually, HD calculates the number of transitions of 0 and 1 in a register, which is equivalent to HD(d_1,d_2) = HW($d_1 \oplus d_2$) , where d_1 represents the data in a register before the value changes, d_2 represents the data in a register after the value changes and $\oplus$ represents the XOR operator.

The attack is performed on the 10^{th} round input of the AES with an aim to retrieve its round key. In order to recover the key, an attacker performs the round operations in an inverse manner, as represented in figure 4.3(a). The corresponding power trace samples are stored in the form of a matrix whose elements are represented by equation 4.1:

$$v_{i,j} = SBox^{-1}(ShiftRows^{-1}(k_{i,j} \oplus c_i)) \tag{4.1}$$

The hypothetical power values are denoted by equation (2):

$$h_{i,j} = HD(v_{i,j}, c_i) = HW(v_{i,j} \oplus c_i) \tag{4.2}$$

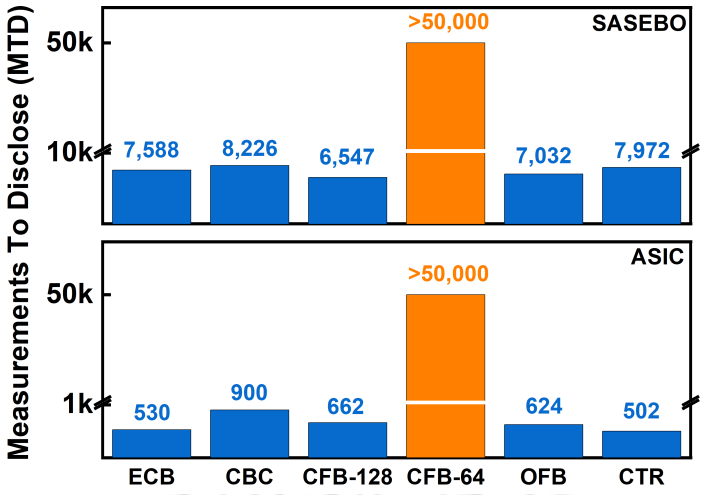
where 'v' is the 10^{th} round AES input, which is a function of $f(c, k)$, 'c' is the ciphertext,'k' represents the last round key values, 'i' in equation 4.1 and 4.2 represent the plaintexts, 'j' in equation 4.1 represents the samples of the obtained trace and it represents the possible key bytes in equation 4.2.

The similarity in the last round operations of CBC with ECB allows the conventional attack model to be used for the former. However, the 10^{th} round AES output is XORed with the plaintext to finally obtain the ciphertext for CFB, OFB and CTR modes. This necessitates a new attack model for these modes wherein the only addition has to be a 128-bit XORing between the plaintext and ciphertext. Although this step might seem trifle, it is impossible to obtain the keys of CFB, OFB and CTR modes, if not incorporated. Figure 4.3(b) illustrates the proposed attack model with the new integration. Hence, equation 4.1 gets modified accordingly, as represented in equation 4.3, whereas, $h_{i,j}$ remains same as equation 4.2 for the proposed model, with the attacker having the knowledge of c_i and p_i. The corresponding representation of this proposed model is represented in Figure 4.3(b).

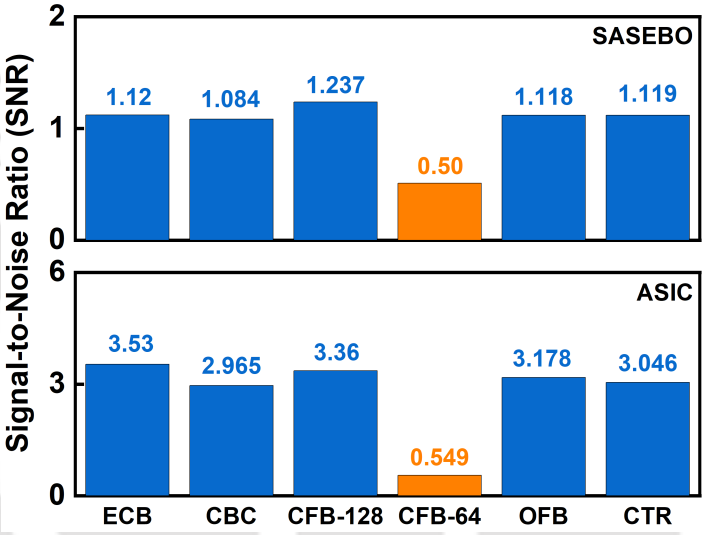
4.3 Novelty of the proposed architectures

AES designs, in general, are operated in the ECB mode owing to its easy design architecture. Literature depicts very few works paying attention to the AES mode of operation as the primary understanding is that the modes are employed to facilitate parallel processing of data. However, it is worthy to note that any design step in AES is expected to have an effect on the security imparted. In the first place, to ensure its candidature for usage in IoT hardware, the standard modes of operation defined by NIST is converted to a rolling architecture, thereby saving immense area and power in operating AES. The hardware-suitable rolling architectures of the modes are represented in Fig. 4.1. Secondly, with the usage of additional inputs, such as, Initialization Vector or Counter, tapping the intermediate outputs of the mode to serve as input for the next plaintext run, and bit selection policy, it is obvious that these steps will impact the security offered by AES run in various modes of operation. From the architectural definition, the non-feedback modes, ECB and CTR, have a direct relation between the plaintext and its ciphertext, hence it is bound to be weak towards the attacks. Amongst the feedback modes, CBC, CFB and OFB, the only one whose AES output does not directly serve as the input to the next AES run is CFB. Hence, it was instinctively expected that CFB would turn out to be the most secure among all the modes. An additional feature in CFB was the bit selection policy which allowed to select only a particular set of bits, 1, 8, 64 and 128, in the intermediate operations with a boundation for the plaintext to match this size. Hence, to process the standard 128-bit plaintext, it would require 128 clocks if the selection policy selected 1 bit out of the intermediates. On the other hand, selection of 128-bit would imply no bits neglected resulting in higher correlation between the processed plaintext and its corresponding ciphertext. So, an optimal choice was the selection of 64 bits which implied inconsideration of 64 bits, and requiring 2 clocks to process the standard 128-bit plaintext data, as represented in Fig. 4.2.

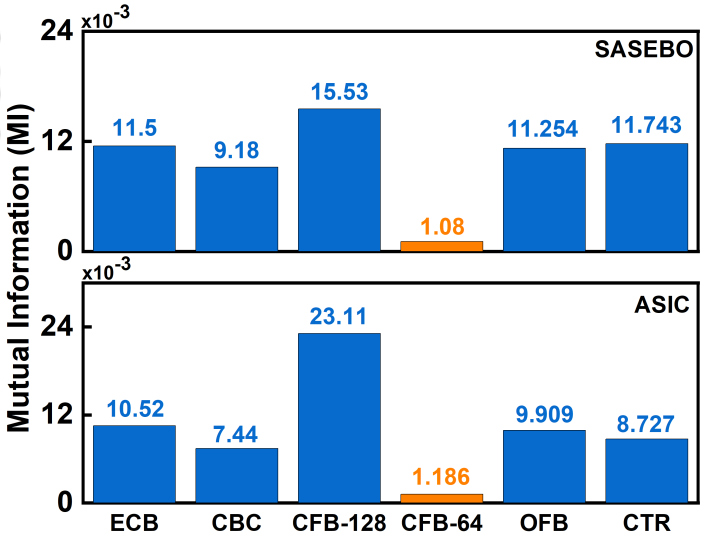
Another important aspect of our novel work is that the standard CPA attack model which was discovered to attack only ECB mode, has been modified and made adaptable for attacking every mode of operation. It is conclusive that the standard attack model can never successfully attack the modes of operation other than the ECB mode, as the point of attack (AES last round) varies for every mode.



(a) MTD comparison



(b) SNR comparison



(c) MI comparison

Figure 4.4: Hardware security metrics comparison for all the modes on SASEBO and ASIC

Power in the range of μW is achieved owing to the way the circuit is designed. Instead of replicating the AES block as suggested by NIST, the implementation is done in 12 clocks by employing rolling architecture which minimizes the area, which in turn reduces the power. Also, the design ensures operation of each AES round in a single clock, thereby ensuring that the critical path is reduced, hence the delay incurred is in terms of ns.

4.4 Hardware security metrics evaluation

The aforementioned models are utilized to evaluate the resilience of the AES modes using the security metrics. As discussed, the conventional attack model is used to attack the ECB and CBC mode designs, whereas the proposed attack model is used to attack the CFB, OFB and CTR mode designs, including the proposed mode. As stated in the previous section, usage of the conventional attack model on the latter designs is expected to be futile. This section intends to check the trend of the security offered by the designs under consideration, and eventually test the resilience of the proposed mode.

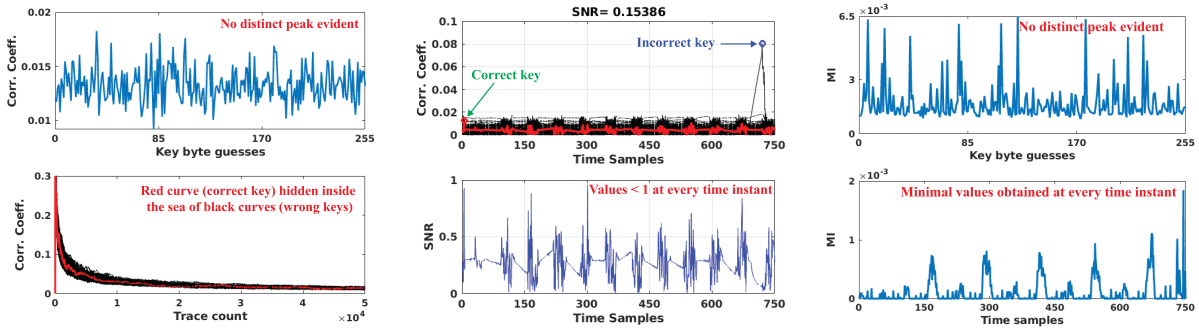
4.4.1 Security metrics' trends depicted by the investigated modes

The modes of operation under investigation are evaluated for their security metrics on ASIC and SASEBO platforms. The key recovery attacks are performed for every byte of all the designs. The byte with the 'highest' MTD in each mode is represented in the MTD plot in figure 4.4(a). On SASEBO, all the modes break down before 9,000 traces whereas the proposed CFB-64 mode withstands the attack for more than 50,000 traces. ASIC results, although are on similar lines, the key gets recovered way before mere 1,000 traces. The reason behind early recovery of the cipher key is that the ASIC environment of power traces generation is an ideal one whereas that of SASEBO contains non-idealities contributed by the components on the board. Another noteworthy point from the MTD comparison is that the CFB, OFB and CTR mode designs are successfully cracked using the proposed attack model which would have not been possible with the conventional CPA attack model. This justifies our proposal to be a valid one.

Contrary to the MTD comparison, the byte with the 'least' SNR in each mode is chosen for the SNR comparison, as depicted in figure 4.4(b). All the modes, except CFB-64, show SNR values > 1 on SASEBO as well as ASIC platforms. This designates the proposed CFB-64 mode to be non-leaky of side-channel information to the attacker whereas the other designs are quite leaky in nature. Finally, the comparison of MI values with the byte which has the 'lowest' MI in each mode is shown in figure 4.4(c). Similar to SNR, CFB-64 exhibited the least MI value in comparison to other modes on SASEBO and ASIC platforms. From the comparison illustrated in figure 4.4, it can be evidently concluded that the proposed CFB-64 mode offers the highest resilience to all the key recovery attacks performed on it. Not even a single key byte is recovered by employing such attacks with 50,000 plaintexts, signifying the strength of the proposed mode.

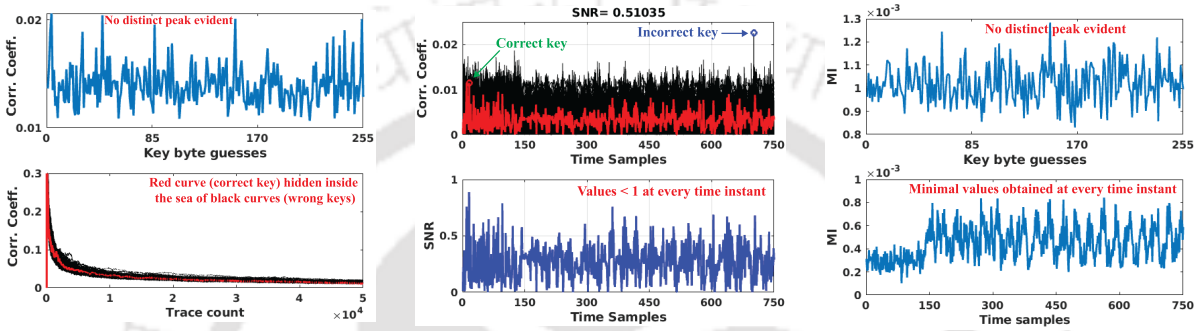
4.4.2 Security metrics evaluation of the proposed CFB-64 mode

The security metrics for the proposed mode are evaluated upon cracking a sample byte of the cipher key, whose results are shown in figure 4.5, 4.6 and 4.7, for ASIC and SASEBO platforms. In the MTD plots depicted in figure 4.6 and 4.7, there is no distinguished peak with a very high correlation score for any key byte guess in the correlation coefficient versus



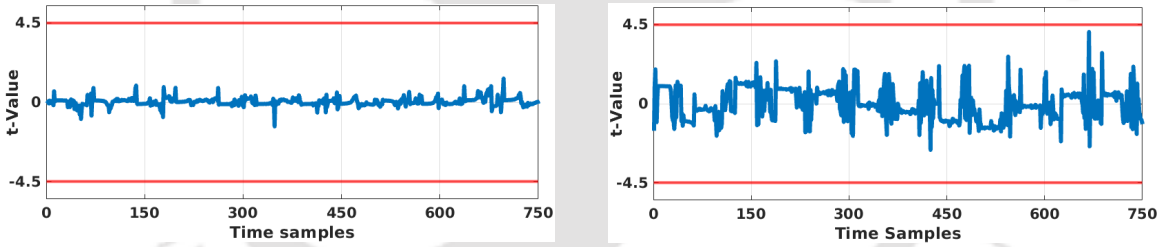
(a) MTD plot (b) SNR plot (c) MI plot

Figure 4.5: ASIC-based security metrics for the proposed CFB-64 mode of operation



(a) MTD plot (b) SNR plot (c) MI plot

Figure 4.6: SASEBO–based security metrics for the proposed CFB-64 mode of operation



(a) ASIC TVLA (b) SASEBO TVLA

Figure 4.7: TVLA plots for the proposed CFB-64 mode of operation

key byte guesses plot, to indicate the successful recovery of the correct byte for the proposed mode. Also, the MTD plot depicting correlation coefficient versus trace count shows failed key recovery even after employing 50,000 plaintexts. In the SNR plots, the SNR values are obtained as a ratio between the correlation coefficient of the correct byte (green bubble) and the highest correlation coefficient amongst the wrong key guesses (blue bubble) in the correlation coefficient versus time samples plot. A higher position of the blue bubble indicates a failed key recovery attempt for CFB-64. Also, the SNR versus time samples plot portray consistent SNR values < 1. Similar to MTD, no key byte guess depicts a distinguished peak in the plot for MI versus key byte guesses for CFB-64. Also, MI values of few milli imply insignificant information being leaked to the attacker [94], which is evident from their time samples plot. Figure 4.7 depicting t-values within the safe levels of in the TVLA plots render the proposed CFB-64 mode to be non-leaky in nature. Comparison of the proposed mode w.r.t. some designs in literature indicated a significant increment in security, as illustrated in

Table 4.3: Proposed countermeasure vs. state-of-the-art designs

Countermeasure design	Overhead (%)		
	Area	Power	Performance
GI [147]♣	42.5	130	20
ASNI [95]♣	60	68	0
SDRR [94]♣	33	180	0
Detection [208]♠	7.2	14.3	0
Proposed$♠	**19.46**	**-19.99**	**-59.97**

$w.r.t. ECB ♣chip-based results ♠simulation-based results

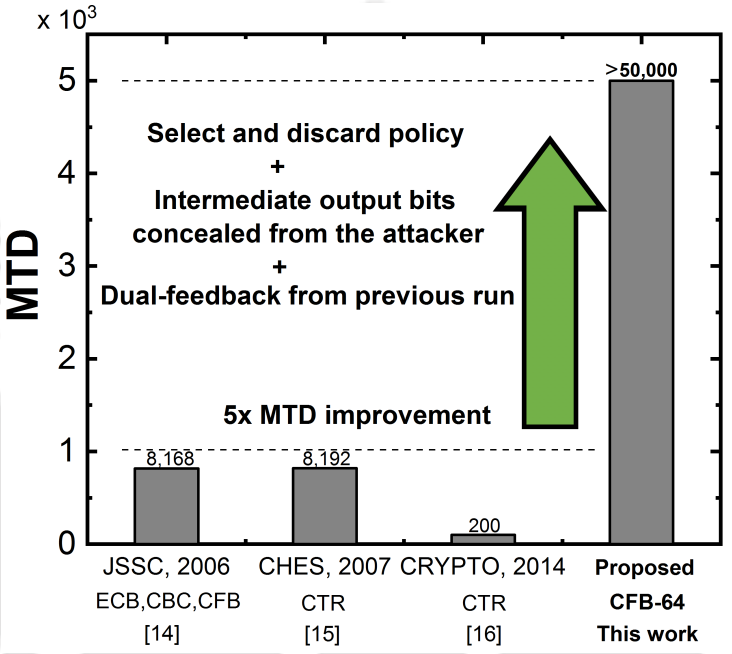


Figure 4.8: Security improvements of the proposed CFB-64 mode

Table 4.3 and Figure 4.8. A clear conclusion can be drawn from the table and the graph that a huge area and power savings can be achieved ensuring a high security using the proposed CFB-64 mode.

4.5 Chapter summary

This work proposes new architectures for the ECB, CBC, CFB, OFB and CTR modes of AES to comply with the stringent area and power constraints of IoT hardware. Since the conventional CPA attack model could only attack the ECB and CBC modes, a new attack model is introduced for the other modes, using which the cipher key is successfully recovered. This work also proposes a novel CFB-64 mode utilizing bit selection policy of an intermediate output, which exhibits the highest security amongst all the modes. By employing the bit selection policy on the output block, it is ensured that the output is partially available to the attacker which makes it difficult to attack on the output block. It is due to the fact that the construction of hypothetical power model requires the availability of both plaintext and ciphertext to the attacker, which is highly difficult to achieve with the proposed mode. As

the crucial 64-bits of the output block are neglected, the statistical analysis of the power attacks for the construction of hypothetical power model is expected to fail. Upon testing on ASIC and SASEBO, the proposed mode withstands an MTD test of 50,000 plaintexts, and depicts an SNR < 1 and minimal MI values in the range of few milli, implying a non-leaky design. With the intrinsic resilience of AES boosted thus far, an actual addition of the countermeasure is expected to occupy minimal area and power overheads.

CHAPTER

5

SPLITTING THE SUBBYTES OPERATION FOR A COUNTERMEASURE EFFECT.

Contents

5.1 Role of SubBytes' round operation in countermeasure design process 72
5.2 SubBytes implementation across multiple clocks 73
5.3 Analyses of the various SubBytes implementation 74
5.3.1 Trace pattern comparison 74
5.3.2 Hardware resources analysis 74
5.3.3 Security analysis of the investigated designs 76
5.4 Proposed clocking strategy 76
5.5 Novelty of the proposed design 77
5.6 Security analysis of the proposed design 78
5.7 Chapter summary 80

Having chosen the Masoleh S-box and designed a novel CFB-64 mode, these two aspects are incorporated into the AES design in this thesis chapter. As evident from the understanding developed from the CPA attack model, a designer's utmost priority is to secure the SubBytes round operation. Although the first involvement between the cipherkey and ciphertext (or plaintext) is the AddRoundKey operation either from the first or last AES' round, the power side-channel information liberated from this operation is not sufficient for an attack. SubBytes, owing to its 75% contribution to the total AES' power consumption, serves as the best point of attack for an adversary. This thesis chapter looks into its various possible implementations with an agenda to ensure lesser power side-channel information is liberated to the adversary. Eventually, a method is proposed depicting optimal hardware resources utilization and the highest security among the considered designs.

5.1 Role of SubBytes' round operation in countermeasure design process

Literature portrays various countermeasure designs suffering from severe area and power overheads. Incorporation of such bulky countermeasures into AES may not make it permissible for usage in resource-constraint IoT edge devices. With technology competing to produce rapid results, one of the prime reasons for countermeasures bearing huge overheads is the AES being used as low latency designs in the form of a 12-clock or a 14-clock implementation. In such designs, the SubBytes comprising of 16 S-boxes is executed in a single clock. The compensation for such fast designs is paid in the form of immense power release owing to 16 S-boxes operating in tandem. The significance of this point can be understood by the fact that 3,504 logic gates are in operation at a time (16×219 gates per Masoleh S-box). In order to hide the effect of such a power-dominant AES round operation, a countermeasure with comparable or significantly greater power is required to suppress the power side-channel information. In the quest to meet such requirements, designers tend to devise wrappers to shield such leakage effects. Integrated, on-chip and inductive voltage regulators, signature attenuation circuits, switched capacitor-based time varying transfer function, Low Drop Out (LDO) regulator, random fast voltage dithering circuits, power management circuitry, etc. are some aspects exploited to shield SubBytes-related information from reaching the adversary. However, these countermeasures suffer from immense area and power overheads potentially disqualifying them from being integrated into an IoT edge device.

It is to be noted that AES developers intended SubBytes to provide nonlinearity and confusion to the data being processed by it. Undoubtedly, the SubBytes-processed output is distinctively different from its input, however it has an adversarial impact in the form of information leakage. Taking a leaf out of the AES design principle, the adversaries, very intelligently, transformed the strongest aspect of AES, i.e., the SubBytes, into its weakest point by making it the point of PAAs. They plainly utilized the fact that SubBytes is the most power consuming AES round operation. Hence, it's essential that an AES designer puts on the same cap as the attacker while devising any countermeasure strategy. This thesis work investigates splitting the SubBytes round operation across multiple clocks with a target to minimize information leakage. The most important advantage out of this exercise is that upon designing an actual physical countermeasure circuit, it needs to take into account the effect of a lesser number of S-boxes to be shielded. This will result in a small-size countermeasure with minimal overheads and enhanced security. It can be considered as another attempt to boost the AES' intrinsic security so that the countermeasure designs may receive less effort.

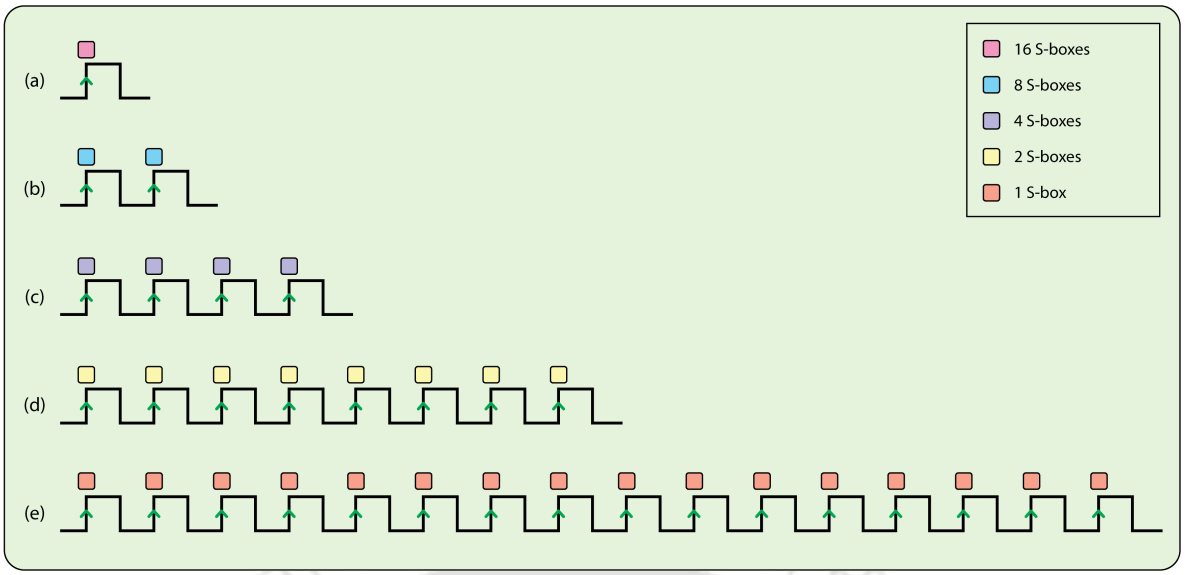


Figure 5.1: Illustration of SubBytes implementation across multiple clock cycles (a) 1-clock, (b) 2-clock, (c) 4-clock, (d) 8-clock, (e) 16-clock implementation

5.2 SubBytes implementation across multiple clocks

With the SubBytes round operation serving as the platform for CPA attack model, its implementation across multiple clock cycles is studied. The motive is to minimize the side-channel leakage by performing lesser S-box operations at a time. Figure 5.1 illustrates the investigations undertaken for the study. A 1-clock SubBytes implementation involves 16 S-boxes operated in a single clock, and a 2-clock SubBytes implementation employs 8 S-boxes executed in a single clock, thus needing 2 clocks to complete the 16 bytes substitution. A 4-clock Subbytes implementation has 4 S-boxes working in each clock, whereas an 8-clock design entails 2 S-boxes every clock. Finally, a 16-clock design has a single S-box implementation every clock cycle. From this illustration, we can be sure that the power leakage will be less in split-SubBytes implemenation (Figure 5.1 (b)-(e)). Comparatively, Figure 5.1(e) is expected to deliver the least information to the attacker owing to its single S-box usage. It is to be noted that in this case, "only 1 S-box is reused" in the design every clock cycle thereby bringing a drastic decrement in the hardware consumption, compared to the conventional usage of 16 S-boxes in 1-clock implementation. Undoubtedly, the throughput is compromised owing to the large latency of the design. However, the split-SubBytes designs are expected to possess throughput good enough for IoT applications which do not demand extremely high throughput. Similar to the 16-clock implementation, 2 S-boxes are reused in 8-clock design, 4 S-boxes are reiterated in 4-clock design and 8 S-boxes are recurrent in 2-clock SubBytes implementation, every clock cycle.

A noteworthy point to be made here is that although significant hardware is reduced by reusing S-boxes, say in 16-clock implementation, there is a slight increment, too, in the form of addition of registers to hold partial outputs every clock cycle. In all the cases represented in Figure 5.1, it is to be ensured that the AES round output is to correct. The representations in the figure are pertaining to only one round operation resulting in 12-clock, 22-clock, 42-clock, 82-clock and 162-clock complete AES design implementation for 1-clock, 2-clock, 4-clock, 8-clock and 16-clock SubBytes implementation, respectively.

Table 5.1: Hardware resources comparison of various clocking strategies on ASIC and FPGA

AES design	Area (μm^2)	Power (μW)	Delay (ns)	Throughput (Gbps)	Figure of Merit (FoM) ($\times 10^{25}$ bps/μ^2W)
12-clock	12,705.48	98.41	3.63	2.938	0.157
22-clock	14,546.52	78.5187	3.84	1.512	0.105
42-clock	13,538.52	79.6896	3.84	0.787	0.062
82-clock	13,474.44	83.4597	3.86	0.436	0.054
162-clock	14,290	92.5282	3.84	0.206	0.028
Proposed design	16,822.44	85.2891	0.9	1.734	24.171

5.3 Analyses of the various SubBytes implementation

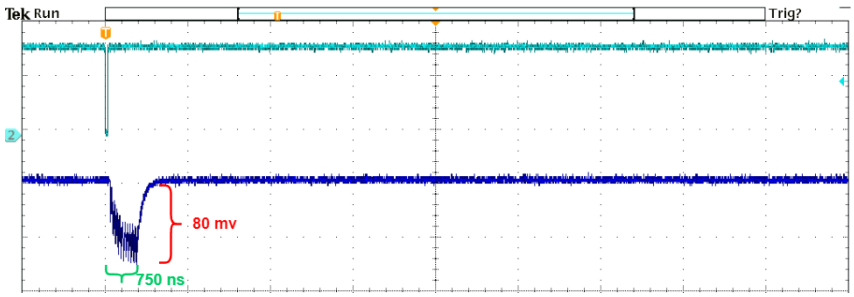
The aforementioned designs are investigated for their hardware resources utilization and offered security so that they can serve as the basis of addition of an actual countermeasure circuitry. The first step is to scrutinize the power trace patterns in order to confirm if the assumptions made in the previous sections are actually practically observed. Henceforth, the hardware resources are probed to opt for a design as the final choice.

5.3.1 Trace pattern comparison

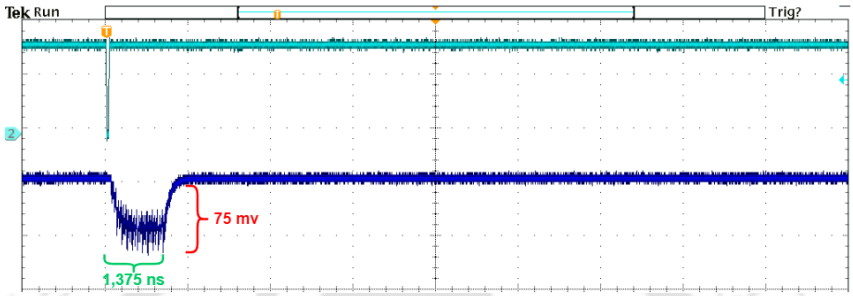
In order to verify the sought power minimization effect for an AES design, the strategies illustrated in figure 5.1 are implemented on SASEBO to check for their trace patterns. As expected, the switching magnitude reduces as we go from a 12-clock design to a 162-clock design, as portrayed in Figure 5.2. The latency of the designs is also evident in the depicted trace patterns. In terms of the power side-channel leakage, it is expected that the 12-clock AES implementation leaks the most side-channel information owing to the large power magnitude depicted in the trace waveform pattern. In contrast, the 162-clock clock design which consumes very minimal power every clock cycle owing to its single S-box implementation, is expected to liberate the least side-channel information to an adversary. It is very conclusive from the figures that a countermeasure will require a large hardware to ensure enough power is released to suppress the power signature of the 12-clock AES design. However, for a 162-clock design, the task is extremely simplified, as the countermeasure needs to overpower only a single S-box, which is a lot easier task expected to consume very less area and power.

5.3.2 Hardware resources analysis

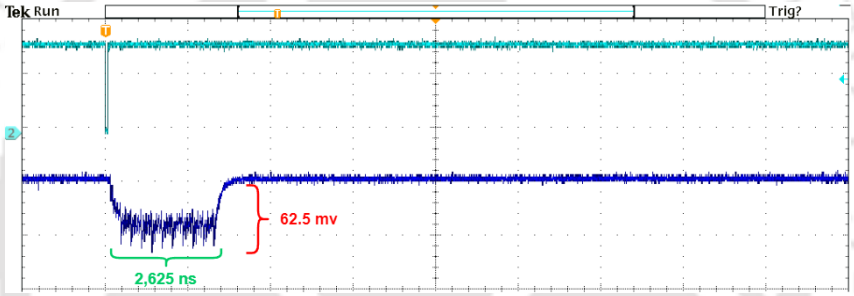
The considered designs are synthesized using Synopsys Design Compiler using UMC 65 nm technology node whose results are tabulated in Table 5.1. The information pertaining to the proposed design and Figure of Merit (FoM) will be discussed in the subsequent section. The considered designs consume comparable area and power, with a steady decline in throughput observed due to the increased clock utility in the designs. It is to be noted that the power value represented here pertains to the power consumed by the total circuit wherein apart from the SubBytes-dissipated power, circuit components such as registers contribute a huge share. Hence, the highest power drawing 12-clock design can be attributed to all the S-boxes being processed in a single clock cycle, whereas the second highest power consuming 162-clock design can be accounted for its excessive register usage for a high latent design.



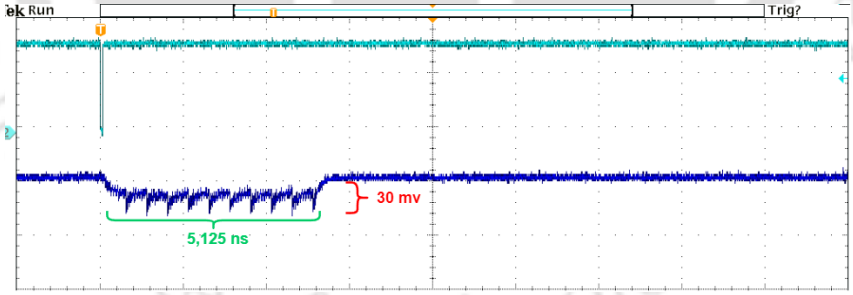
(a) 12-clock AES design with 1-clock SubBytes implementation



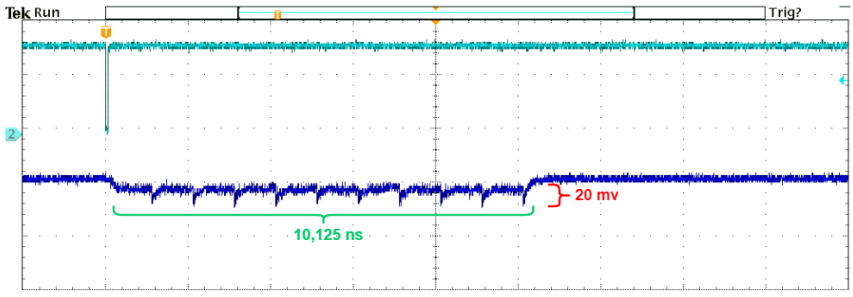
(b) 22-clock AES design with 2-clock SubBytes implementation



(c) 42-clock AES design with 4-clock SubBytes implementation

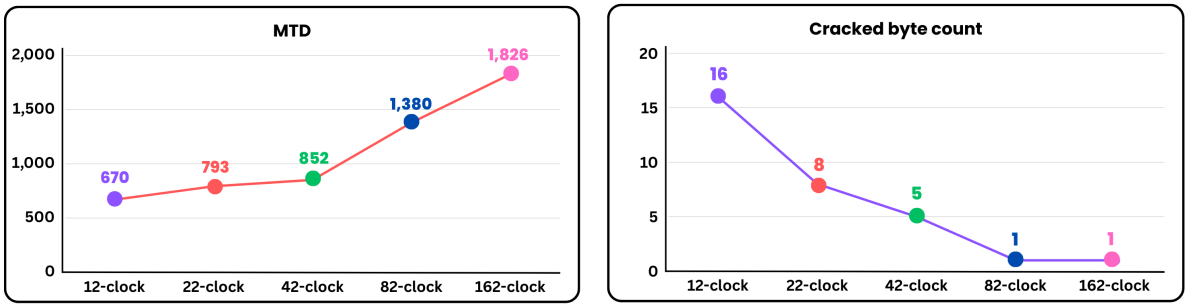


(d) 82-clock AES design with 8-clock SubBytes implementation



(e) 162-clock AES design with 16-clock SubBytes implementation

Figure 5.2: AES trace comparison for SubBytes implementation across different clock cycles



(a) MTD comparison on ASIC

(b) Cracked bytes comparison on SASEBO

Figure 5.3: Security comparison of the investigated designs

5.3.3 Security analysis of the investigated designs

Having observed their resources consumption data, a security analysis of the surveyed designs is performed to check for their resilience towards CPA attacks on both ASIC and SASEBO platforms. Upon using 10,000 plaintexts to crack the AES cipher key on ASIC, all the bytes got cracked for every design, as shown in Figure 4.3(a). The credit to such a result can be attributed to the ideal (noiseless environment) power traces generated. As claimed, that 162-clock AES design implementation is expected to liberate the least power side-channel information, it exhibited the highest MTD of 1,826, followed by 82-clock AES design. The least MTD is depicted by the 12-clock design with the highest switching magnitude in its power trace pattern. Upon using the same 10,000 traces to attack the investigated designs on SASEBO, not all the bytes got cracked for all the designs. Hence, a comparison is made between the number of bytes getting cracked for every design, as represented in Figure 4.3(b). The 12-clock design has all its bytes cracked whereas only 1 byte could be recovered for both, 82-clock and 162-clock AES designs.

With irregularities in the trend of values observed for area and power, a common basis is used in the form of Figure of Merit (FoM) for a fair comparison. It is defined by taking the ratio of parameters with desired higher values w.r.t. the parameters with desired lower values, as represented by equation (5.1).

$$FoM = (MTD \times Throughput)/(Area \times Power) \tag{5.1}$$

The FoM trend depicts that, with increment in clock cycles for its implementation, an AES design becomes less efficient considering all the resources as well as security aspects. This arises the need for an optimization or wise design choice to balance security with latency.

5.4 Proposed clocking strategy

Having examined the security aspects and hardware resources utilization, it is quite evident that 82-clock and 162-clock design are the best candidates out of the lot. However, with the alarming FoM, it necessitates a wise design strategy to utilize the concept of "SubBytes splitting" without compromising on the FoM. Hence, a novel clocking strategy is proposed where an 82-clock design is utilized like a 162-clock design by catching hold of both the positive and negative clock edges, and running (basically, reusing) only 1 S-box at a time. Figure 5.4 depicts the same with a green-colored positive-edge (posedge) and a red-colored negative edge (negedge) highlighting a single S-box implementation every clock edge.

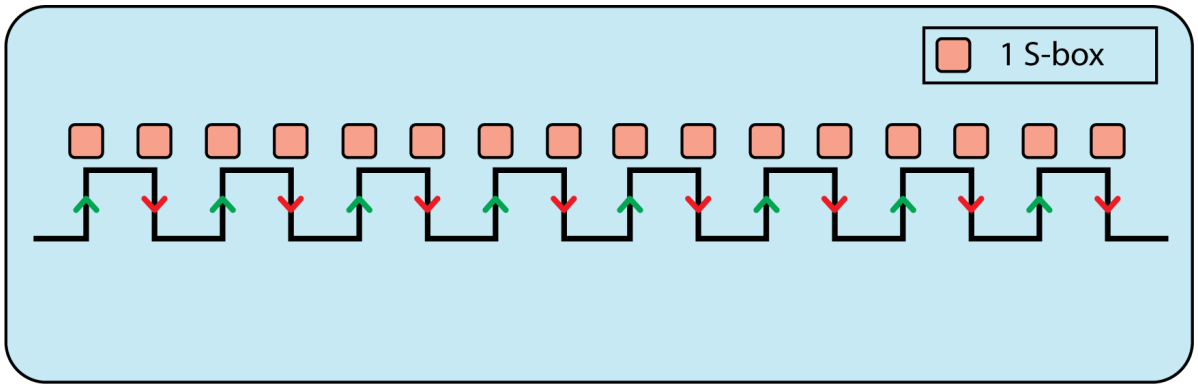


Figure 5.4: Proposed clocking strategy utilizing posedge and negedge in an 82-clock design

The proposed clocking strategy very wisely ensures that latency is saved by half by transforming the 82-clock design to a 162-clock one to achieve the latter's security at the cost of the former's latency itself. A look at the Table 5.1 indicates that it has an area increment of 17%, however enjoys power decrement of 7.82% and throughput increment of 8.4× w.r.t. the 162-clock design. FoM is extremely high for the proposed design.

5.5 Novelty of the proposed design

The prime focus of AES designs, as laid out at the outset of the thesis, has been area minimization by reducing the gate count of the overall design. To be suitable for resource-constraint IoT edge devices, power was another parameter which caught the attention of researchers, gradually. However, due to the accessibility of these devices, they are prone to power side-channel attacks with the AES SubBytes round operation drawing 75% of the total power. Adversaries particularly attack this operation to siphon off critical information about the data processing in the algorithm which necessitates dire attention towards it. A straightforward observation is that if an AES design has to be secured using a countermeasure, the latters power has to overcome the effect of the whole SubBytes operation running sixteen S-boxes in parallel over a single clock edge. Hence, the proposed work intends to diminish the side-channel information per clock edge by splitting the sixteen S-boxes over eight clocks and utilize both the edges to execute a single S-box every edge. By utilizing both the positive and negative clock edges, a latency saving of 2× is achieved, else the design would have been implemented in 16 clock cycles instead of 8. The main target of this work is to devise an extremely lightweight countermeasure which would require to overpower only a single S-boxs effect towards side-channel information, and not the whole set of 16 S-boxes. Another remarkable novelty of this clocking scheme proposal is that unlike the conventional AES implementations where sixteen S-boxes are used, only a single S-box is reused at every clock edge to fulfil the SubBytes round operation thereby immensely saving area and power.

The comparison table, Table 5.2, clearly shows an immense decline in area and power consumption owing to the proposed clocking scheme adopted to implement the SubBytes round operation. There is a compromise in throughput owing to the usage of more number of clocks to execute the SubBytes round operation. However, the trade-off in performance is compensated by the security this design style offers, because a very small countermeasure will be sufficient to overcome the effect of a single S-box leaking side-channel information. A noteworthy point is that despite the loss in performance, the overall throughput of the

Table 5.2: Proposed countermeasure vs. state-of-the-art designs

Design	Technology	Area (mm^2)	Power (μW)	Performance loss
GI [147]♣	40 nm	0.0456	23,000	-
ASNI [95]♣	130 nm	0.43	1,680	0%
SDRR [94]♣	65 nm	0.055	-	0%
Detection [208]♠	45 nm	0.35	33,320	0%
Proposed[$]♠	**65 nm**	**0.017**	**85.29**	**-40.98**

[$]w.r.t. ECB ♣chip-based results ♠simulation-based results

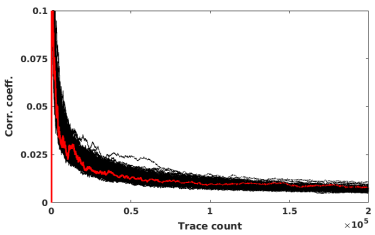
proposed design is 1.734 Gbps. With the throughput requirement of IoT standards, such as, Bluetooth, RFID, Zigbee, WiFi, 3GPP standards, non 3GPP standards, in the range of Mbps, the achieved throughput deems totally fit to be used for these applications.

5.6 Security analysis of the proposed design

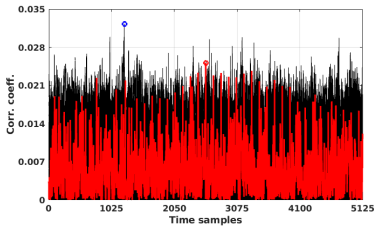
Having examined closely, how security can be improved without compromising on latency, the proposed clocking strategy incorporates the effects contributed by thesis chapters 1 and 2. The Masoleh S-box is utilized along with the novel CFB-64 mode in the proposed pos-neg 82-clock design, with all three of them acting as measures to improve the intrinsic resilience of AES. The conglomerated design is tested against 2 lakh traces using the CPA attack model which failed to recover any key byte. All the security metrics evaluated for sample byte 16 are depicted in Figure 5.5 and Figure 5.6.

As a part of the MTD plot, the correlation coefficient vs. trace count depicts the red curve corresponding to the correct key to be immersed in the sea of black curves, for both SASEBO and ASIC platforms. Also, the correlation coefficient vs. key byte guesses doesn't depict any distinct peak to indicate successful key recovery. For the SNR plots, the correlation coefficient vs. time samples graph indicate the blue-circle (pertaining to the highest correlation coefficient of the wrong keys) to be higher than the red-circle (pertaining to the highest correlation coefficient of the correct key) indicating failed key recovery attempt. Also, the SNR vs. time samples plot doesn't shown any sample value > 1 towards the last round (samples 4,625 - 5125). The MI vs time samples plot revealing information about MI between the real and hypothesis power values range in terms of few milli indicating less information leakage. Similar to MTD, the MI vs key byte guess doesn't show any key byte guess distinctively higher than the rest. Finally, the TVLA plots in Figure 5.7 pertaining to the last round samples indicate all the values to be within the desired range of $-4.5 \geq t \leq +4.5$, thereby referring to the design being non-leaky towards adversaries.

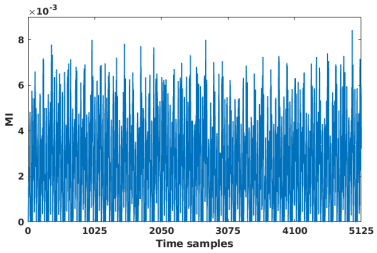
Thus, the amalgamation of the proposed clocking strategy for SubBytes with Masoleh S-box and novel CFB-64 can be considered to be hugely resilient to PAAs, as proven by MTD, SNR, MI and TVLA. The noteworthy point is that all the design steps considered till now has been involving the internals of AES only, ranging from wise choices of an S-box to tweaking the existing modes of operation to a new one, and finally, slowing down the AES operation to boost its resilience.



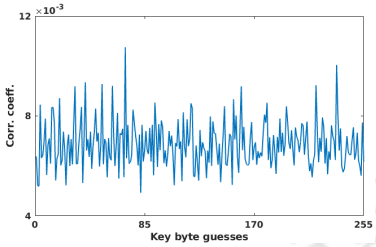
(a) Corr. coeff. vs. Trace count



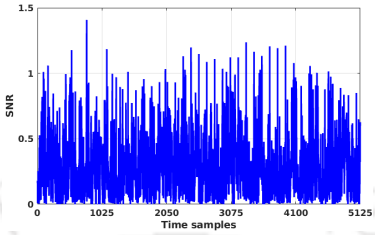
(b) Corr. coeff. vs. Samples



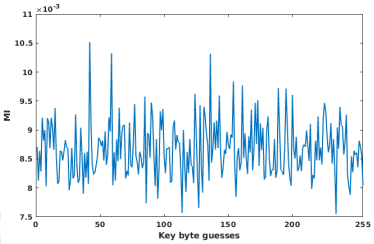
(c) MI vs. Time samples



(d) Corr. coeff. vs. Byte guess

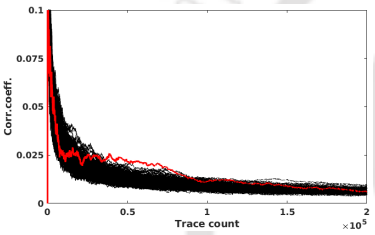


(e) SNR vs. Time samples

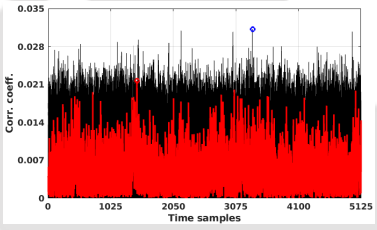


(f) MI vs. Byte guess

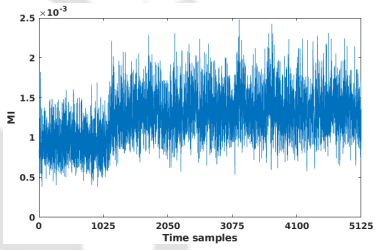
Figure 5.5: ASIC-based security metrics for the proposed pos-neg clocking strategy



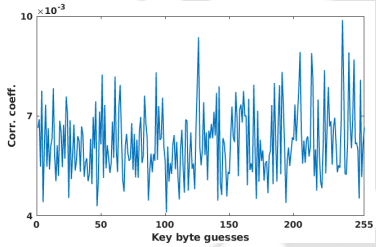
(a) Corr. coeff. vs. Trace count



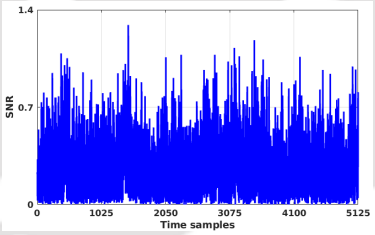
(b) Corr. coeff. vs. Samples



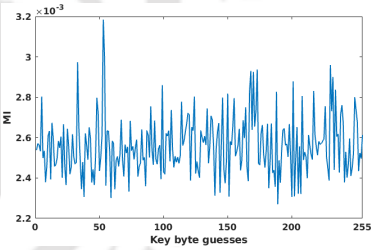
(c) MI vs. Time samples



(d) Corr. coeff. vs. Byte guess

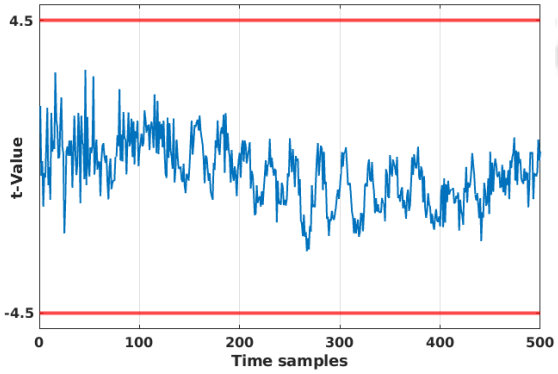


(e) SNR vs. Time samples

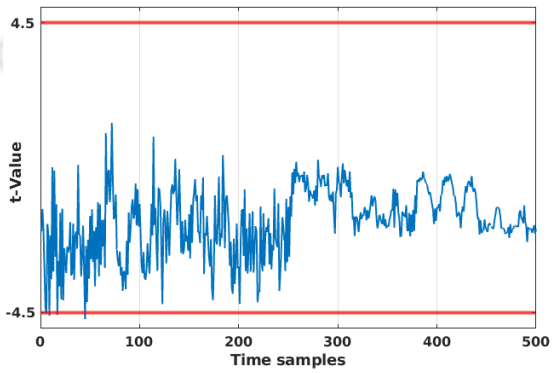


(f) MI vs. Byte guess

Figure 5.6: SASEBO-based security metrics for the proposed pos-neg clocking strategy



(a) ASIC TVLA



(b) SASEBO TVLA

Figure 5.7: TVLA plots for the proposed pos-neg clocking strategy

5.7 Chapter summary

This thesis chapter takes another shot at amplifying the intrinsic resilience of AES by splitting the all-important SubBytes round operation into multiple clock cycles. Upon investigation of various cases employing 1-clock, 2-clock, 4-clock, 8-clock and 16-clock SubBytes implementation, it is evident that the 8-clock and 16-clock SuBytes implementation offered higher security. A proposed strategy utilized the 8-clock SubBytes design in the form of 16-clock by catching hold of both the positive and negative edges of the clock. A latency of 2× is thus saved without compromising on security. To the proposed design, findings from Chapter 1 and 2 are added and its security analyzed. The security metrics suggest that the key bytes could not be cracked even with 2 lakh plaintexts which is a very high resilience for an unprotected design.

CHAPTER

6

COMPRESSION AND EXPANSION-BASED COUNTERMEASURE DESIGN ASSISTED WITH BUFFER DELAYS

Contents

6.1 Countermeasure design strategy 82
6.1.1 Disturbing the AES' power trace amplitude 82
6.1.2 Attempt to disorder the timing of SubBytes operations 84
6.2 Trace pattern analysis 85
6.3 Novelty of the proposed design 87
6.4 Security metrics analysis 87
6.5 Comparison with state-of-the-art designs 89
6.6 Chapter summary 91

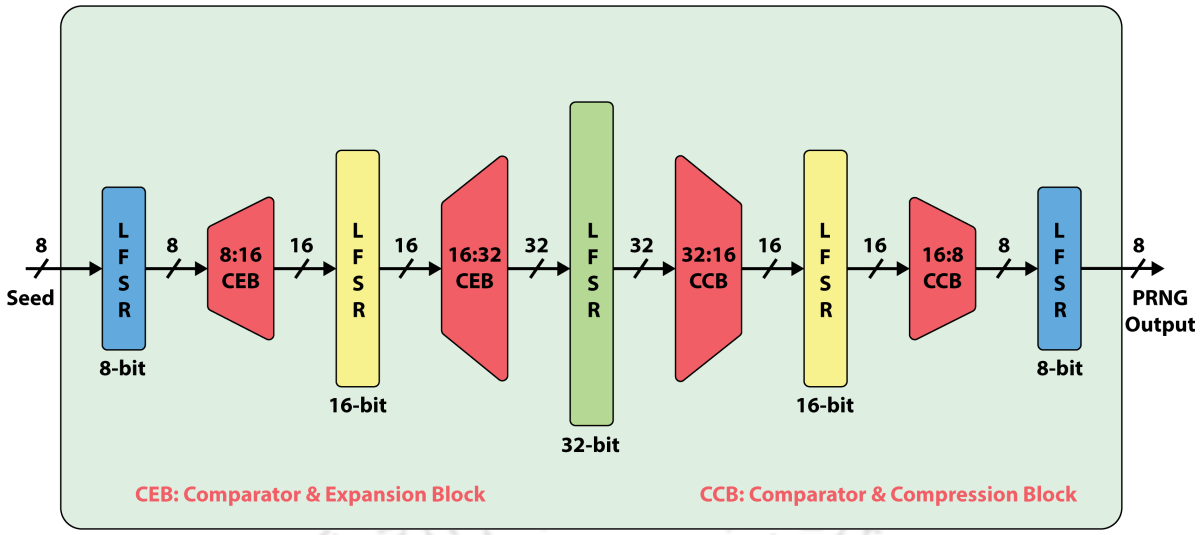


Figure 6.1: Proposed countermeasure based on compression and expansion

Having boosted the intrinsic resilience of AES to a great extent, the actual countermeasure can be planned for its amalgamation with the current state of the AES design. It refers to a design with Masoleh S-box, novel CFB-64 mode and 82-clock pos-neg clocking strategy. The ultimate aim of this thesis, as claimed at the very outset, is to design a countermeasure ensuring minimal area and power overheads without compromising on security. Countermeasures in literature have depicted targeting the power amplitude as well as the time domain for its safe functioning. The ones targeting power amplitude basically tend to disrupt the power trace signature pattern or flatten it so that the variations in the AES trace pattern are distinctly different from its actual power signature. The other category targeting the time-domain intends to shift the all-important SubBytes operation from its actual point of execution, as the CPA attack model requires the alignment of samples corresponding to the same operation for different plaintexts.

With this background information, this thesis chapter proposes a countermeasure taking care of both the amplitude and time axis. Its hardware resources utilization and security metrics are studied, and finally, a layout of the design prepared using Cadence Innovus at UMC 65 nm technology node. Finally, the supremacy of the countermeasure over state-of-the-art designs is illustrated for its consideration as a befitting countermeasure to be used for IoT edge devices.

6.1 Countermeasure design strategy

As stated, the countermeasure design involves taking care of both the amplitude and temporal aspects of the power trace. A countermeasure is proposed in this section which exerts disturbances to the SubBytes functionality and is also out of synchronization from its regular execution.

6.1.1 Disturbing the AES' power trace amplitude

Regular countermeasures face a Herculean task to suppress the effect of 16 S-boxes running in a single clock cycle. However, in this case, the task is extremely simplified to overpowering the effect of only a single S-box working every clock edge. Thus, the countermeasure used must be large in size and consuming a great deal of power. A simple yet effective way of

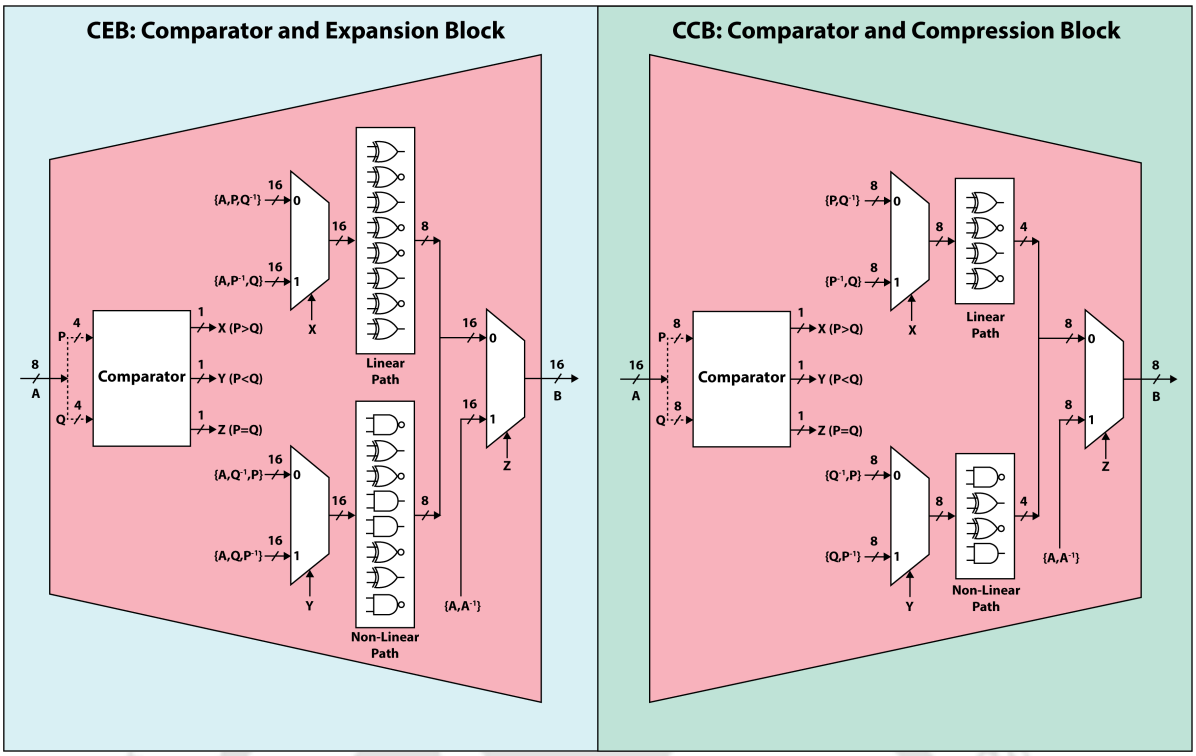


Figure 6.2: Internal structure of 8:16 CEB and 16:8 CCB

marring the power trace is to produce bit flips in addition to the ones involved in SubBytes operation. A Pseudo Random Number Generator (PRNG) is proposed, as shown in Figure 6.1, which works on the principle of expansion and compression of data whose intermediate and final outputs have severe unpredictable switching. The PRNG is laced with an 8-bit LFSR whose output is expanded to 16-bit using a Comparator and Expansion Block (CEB). The CEB output is further randomized with a 16-bit Linear Feedback Shift Register (LFSR) whose output is expanded to 32-bit, using a 16:32 CEB. To add to the randomization, a 32-bit LFSR is employed as an act of randomization. This marks the midway of the countermeasure activity and the intermediate output is now downsized to an 8-bit PRNG output. The 32-bit LFSR output is reduced to a 16-bit value using a 32:16 Comparator and Compression Block (CCB), which is again randomized using a 16-bit LFSR. The randomized output is further down-converted to an 8-bit value with the aid of a 16:8 CCB, and a final randomization is performed using an 8-bit LFSR to eventually produce an 8-bit PRNG output.

Apart from the randomization effect from the LFSR, the CEB and CCB, too, contribute to a great extent owing to its internal operations, illustrated in Figure 6.2. For the sake of understanding, the case of 8:16 CEB and 16:8 CCB is highlighted. The 8-bit input to CEB is split into two nibbles which are compared and depending upon the output of the comparator, the original byte and inverted or usual form of the nibbles are concatenated to form inputs to a mux whose select lines are the outputs of the comparator. The outputs of the muxes whose select lines are X and Y are passed parallelly through some linear and nonlinear gates whose outputs are further concatenated and supplied as an input to the final mux whose select line is the third output of the comparator, Z. The other input to this mux is the concatenated value of the original byte and its inverse. The strategy remains same for the CCB, with the only difference being lesser number of linear and nonlinear gates to downsize the final output.

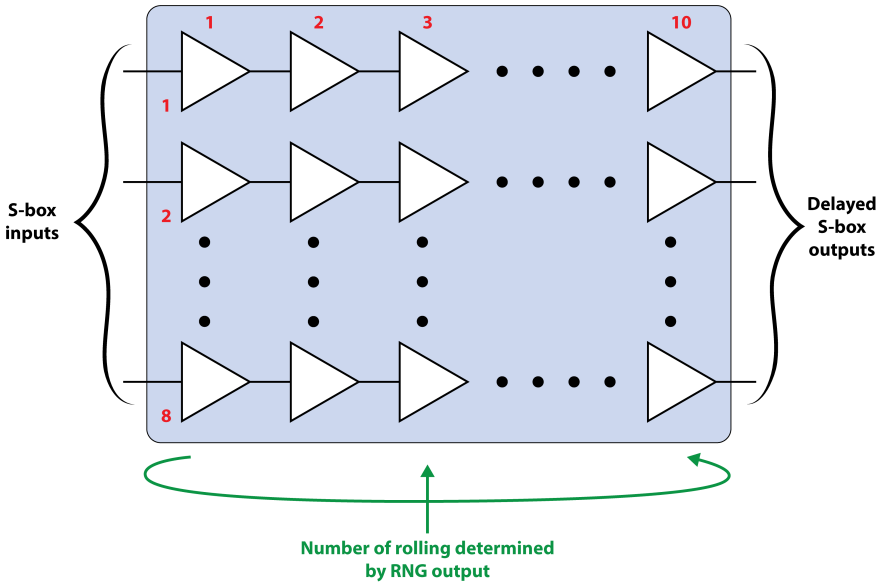


Figure 6.3: Buffer block to delay the S-box operations

6.1.2 Attempt to disorder the timing of SubBytes operations

It is a known practice in digital electronics that the circuits are clock driven, most of which are triggered by the clock edges (positive or negative). Hence, countermeasures where random operations are inserted to dislocate the time instant of Subbytes operation can be aligned by detecting the clock edge. To fail this attempt by the adversaries performing CPA attacks, a buffer-assisted delaying technique is proposed which pushes the S-box execution away from the clock edge by random amount of delay, every clock cycle. The mechanism is represented in Figure 6.3. The synthesis of a buffer depicted a time delay consumption of 0.05 ns, hence 10 buffers for each S-box input offer a block delay of 0.5 ns. This block delay generates different amount of delays triggered by the number of 1s in the PRNG output. Hence, a minimum of 0 1s or a maximum of 8 1s is expected from the PRNG output, implying a minimum of 0 ns delay, or a maximum of a 4 ns delay. It is to be understood that a string of buffers is not used to invoke the delay, rather a single buffer block is rolled multiple times to produce the effect of delay, depending on the number of 1s arriving from the PRNG output. Such a hardware saving act is significant when analyzing the area and power overheads. Thus, the S-box execution is driven away from the clock edge by a random time which is unpredictable for the adversary.

A noteworthy point to be understood is that not all the samples in an AES power trace are actually ‘meaningful’, or contains information useful for the adversary. The CPA attack model clearly indicates that SubBytes is the attack point, and with the divide-and-conquer strategy of recovering the cipher key, byte by byte, samples pertaining to only the S-box execution are actually “meaningful”. Synthesis of an S-box suggests that the time span of an S-box execution is only 3 ns (approximately). Hence, a sampling rate of 1 GSa/s implies only 3 samples per S-box execution are meaningful. With the buffer-based delay, these 3 meaningful samples can go afar from the clock edge by a minimum of 0 ns to a maximum of 4 ns with maximum possibilities of the intermediate delay values like 0.5 ns, 1 ns, 1.5 ns, 2 ns, 2.5 ns, 3 ns and 3.5 ns. With the CPA attack model hugely relying on the trace samples of SubBytes to be perfectly aligned with respect to time during the arrangement

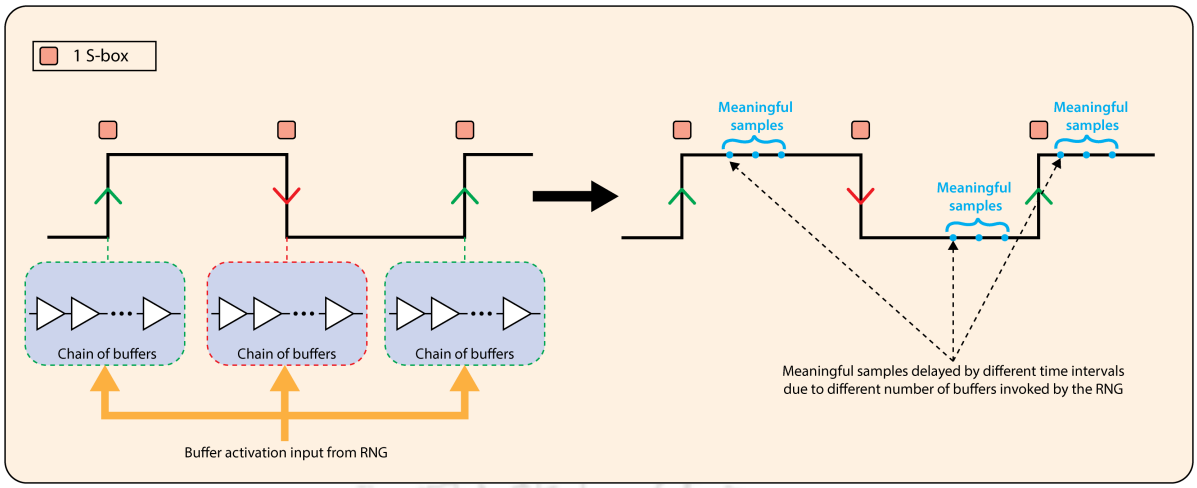


Figure 6.4: Illustration of the effect of buffer-based delays

of their matrices, the disarrayed samples due to the effect of such a buffer action acts as a very good countermeasure. The most important thing is that the hardware expense in such buffer designs is very minimal, with zero power dissipation. Another remarkable act is that an additional circuitry is not required to trigger the buffer blocks, rather the output of the PRNG used to disrupt the amplitude, is reused to save resources.

Figure 6.4 illustrates the aforementioned discussion where a single S-box is represented to be executed every clock edge (both positive and negative). The PRNG output is depicted to trigger the chain of buffers at the clock edges which shows the meaning samples pertaining to S-box operations, drifted from the clock edge by different amount of time. The disarrayed meaningful samples are expected to make life tougher for adversaries, to crack the secret key.

6.2 Trace pattern analysis

The final design of AES, at hand, is a conglomerated version of the thesis chapters 2, 3, 4 and 5, which has an already amplified intrinsic resilience so that the spendings on the actual countermeasure can be minimal. The most important aspect of the design to be tested is that it has been converted from a 12-clock design incorporating an LUT-based S-box to an 82-clock design with Masoleh S-box and novel CFB-64 mode, laced with the countermeasure discussed in the previous section. Also, the effort is to add a small countermeasure which can serve the purpose of shielding the AES from PAAs, sufficient to withstand an attack of 1 million traces. The traces are generated on ASIC and SASEBO platforms by supplying a million plaintexts and recorded for being subjected to the CPA attacks. The security metrics, MTD, SNR, MI and TVLA are subsequently evaluated for both the platforms to justify its resilience.

The layout of the proposed countermeasure design is presented in figure 6.5 which depicts power trace patterns, as depicted in figure 6.6. The layout is marked with areas spanning over the AES with intrinsic countermeasures, such as, the choice of Masoleh S-box, incorporation of CFB-64 mode of operation, and utilizing the split-SubBytes clocking scheme. Also, the proposed countermeasure providing random bit flips and buffer-delay scheme is also highlighted. Their corresponding trace patterns in unprotected and protected form display remarkable difference in terms of the pattern formation, and noisiness. The unprotected trace clearly highlights the processing of five plaintexts with each pattern distinctly highlighted whereas in the case of protected, it is impossible to visually distinctize the processing of

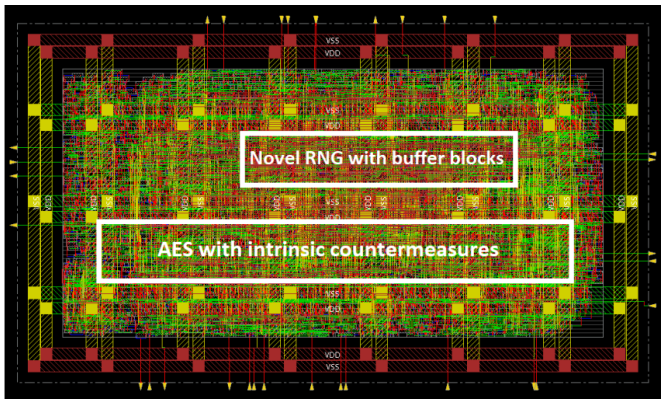


Figure 6.5: Layout of AES after incorporation of the countermeasures

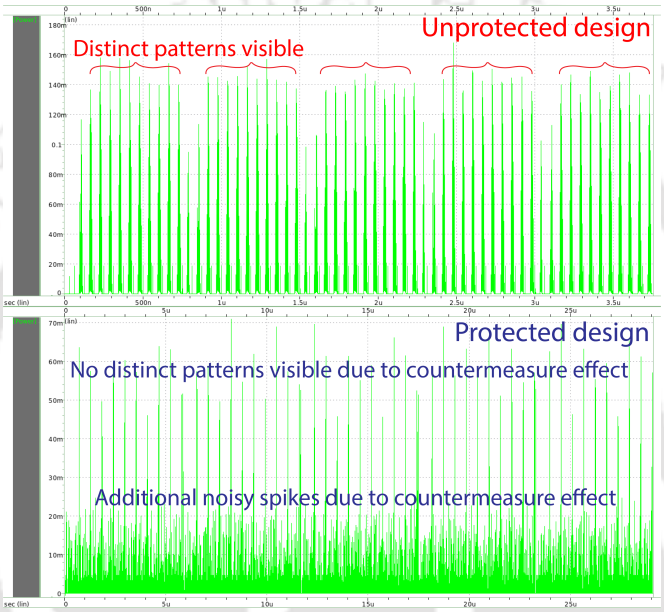


Figure 6.6: ASIC traces of the protected AES design on Synopsys Custom WaveView

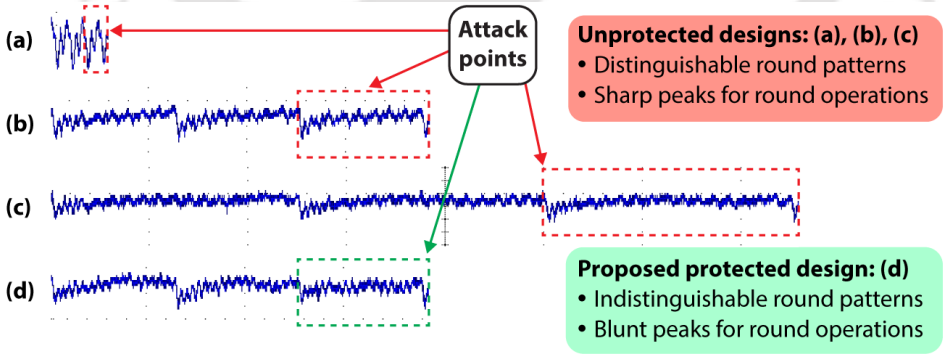


Figure 6.7: Trace pattern of AES after incorporation of the countermeasures

the same five plaintexts utilized for the former case. For the hardware platform, SASEBO, the trace pattern obtained upon processing the countermeasure is depicted in Figure 6.7 which depicts a noisy and an irregular pattern for the round operations. The irregularity and lack of sharp peaks (depicting round operations) indicate successful incorporation of the countermeasure effects.

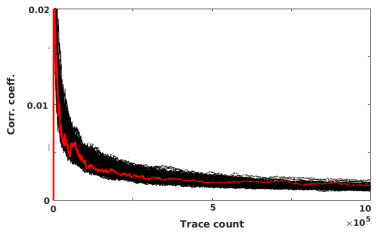
6.3 Novelty of the proposed design

Correlational Power Analysis (CPA) attacks work on the basis of correlating real power traces obtained from an AES design under attack and hypothetically generated power traces for the same set of plaintexts. The attack process necessitates comparison of the power values at the last round of AES for both the sets. State-of-the-art designs primarily focus on trying to break the correlation between the two by adding countermeasure to an unprotected AES and disrupting the power profile. However, the requirement of a successful attack to compare the trace samples for the real and hypothetical power traces for the same set of last round operations go unnoticed. Hence, the proposed countermeasure inculcates both the amplitude and temporal axis properties of a countermeasure to produce a combined effective impact. The most remarkable advantage achieved in this scheme of countermeasure design is that the net effect supposed to be produced by a countermeasure is shared by two different countermeasures, one contributing to the temporal axis, and the other to the amplitude axis. This leads to a very minimal hardware resources spendings, ensuring negligible design overheads.

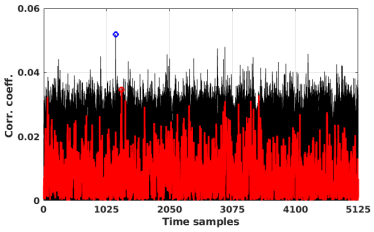
In particular, the proposed countermeasure design utilizes random bit flipping obtained by the actions of CEB and CCB, aided by LFSRs, to disrupt the correlation between power values of the real traces against the hypothetical traces. The temporal aspect is taken care of by delaying the S-box operations at the clock edges by using buffer blocks. The delay generated is random depending upon the RNG output hence making the CPA attack point unpredictable. Another remarkable aspect of the proposed countermeasure is that it was ensured to run for an entire duration of the S-box operation (3 ns) in order to ensure that all the meaningful trace samples collected w.r.t. the operation is corrupted. This observation is important because if the countermeasure extends to only 1 or 2 ns, some samples may carry the side-channel information sought by the attacker. Thus, the proposed design shoulders the amplitude and temporal aspects of a countermeasure design, ensuring negligible overheads with a strong resilience towards CPA.

6.4 Security metrics analysis

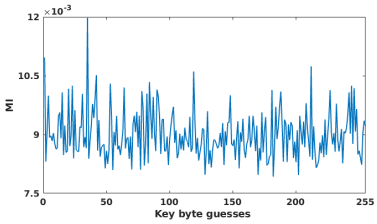
The protected design is being subjected to the metrics analyses whose results are displayed in Figure 6.7, 6.8 and 6.9. As a part of the MTD plot, the correlation coefficient vs. trace count depicts the red curve corresponding to the correct key to be immersed in the sea of black curves, for both SASEBO and ASIC platforms. Also, the correlation coefficient vs. key byte guesses doesn't depict any distinct peak to indicate successful key recovery. For the SNR plots, the correlation coefficient vs. time samples graph indicate the blue-circle (pertaining to the highest correlation coefficient of the wrong keys) to be higher than the red-circle (pertaining to the highest correlation coefficient of the correct key) indicating failed key recovery attempt. Also, the SNR vs. time samples plot doesn't shown any sample value > 1 towards the last round (samples 4,625 - 5125). The MI vs time samples plot revealing information about MI between the real and hypothesis power values range in terms of few milli indicating less information leakage. Similar to MTD, the MI vs key byte guess doesn't show any key byte guess distinctively higher than the rest. Finally, the TVLA plots pertaining to the last round samples indicate all the values to be within the desired range of $-4.5 \geq t \leq +4.5$, thereby referring to the design being non-leaky.



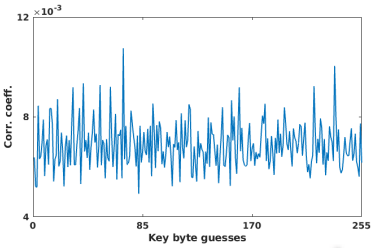
(a) Corr. coeff. vs. Trace count



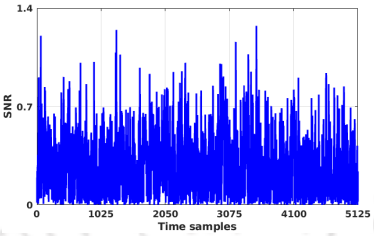
(b) Corr. coeff. vs. Samples



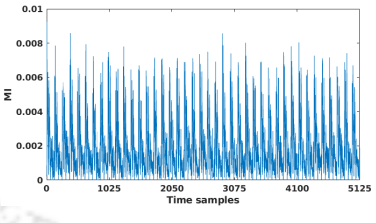
(c) MI vs. Time samples



(d) Corr. coeff. vs. Byte guess

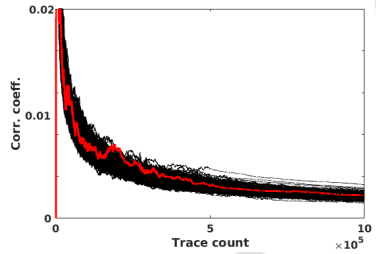


(e) SNR vs. Time samples

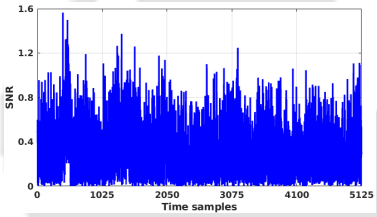


(f) MI vs. Byte guess

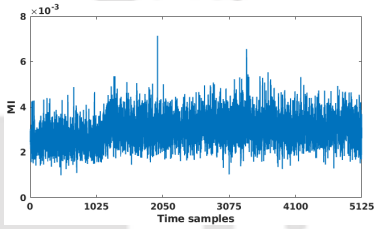
Figure 6.8: ASIC-based security metrics for the proposed countermeasure



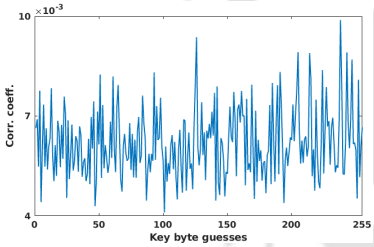
(a) Corr. coeff. vs. Trace count



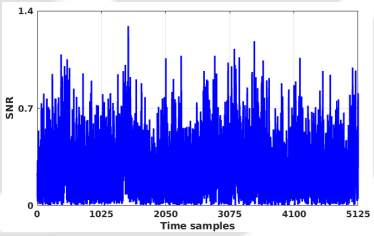
(b) Corr. coeff. vs. Samples



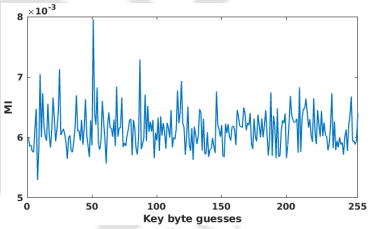
(c) MI vs. Time samples



(d) Corr. coeff. vs. Byte guess

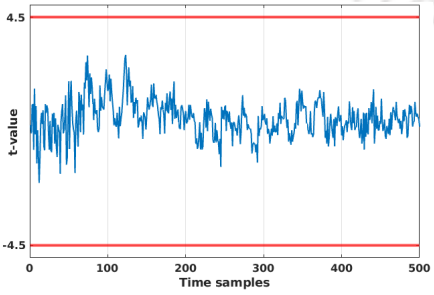


(e) SNR vs. Time samples

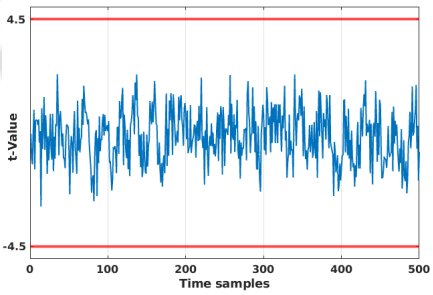


(f) MI vs. Byte guess

Figure 6.9: SASEBO-based security metrics for the proposed countermeasure



(a) ASIC TVLA



(b) SASEBO TVLA

Figure 6.10: TVLA plots for the proposed countermeasure

6.5 Comparison with state-of-the-art designs

Table 6.1: Comparison of the proposed countermeasure w.r.t. state-of-the-art designs.

Countermeasure	**Process**	**Frequency & supply**	**Area** (mm^2)	**Power** (mW)	**Performance** ($Gbps$)
Wave dynamic differential logic (WDDL)[188] ♣	180 nm	50 MHz, 1.8 V	2.45	200	0.99.
Switched capacitor current equalizer [124] ♣	130 nm	110 MHz, 1.2 V	1.37	44.34	1.28
Secure double rate registers[94] ♣	65 nm	20 MHz	0.055	-	-
Digital LDO regulator with SNI & V-REF [83] ♣	130 nm	80 MHz, 0.84 V	0.376	14.388	-
Heterogeneous S-boxes [186] ♣	14 nm	708 MHz, 750 mV	0.3	11	0.845
Non-Linear-DLDO, arithmetic countermeasures [86] ♣	14 nm	-	0.3	-	-
Current-domain signature attenuation [145] ♣	65 nm	50 MHz, 0.8 V	0.205	1.198	-
Digital signature attenuation and time-varying transfer function [8] ♣	65 nm	10 MHz, 0.8 V	0.228	0.284	-
Equalizer LDO [151] ♣	65 nm	3.3 MHz, 0.45 V	0.082	0.0354	-
Syn-STELLAR [152] ♣	65 nm	10 MHz, 0.8 V	0.192	0.2227	-
Proposed countermeasure ♠	65 nm	16 MHz, 1.08 V	0.0229[$]	0.085	1.734

♣chip-based results ♠simulation-based results [$]die area

The most basic way of countermeasure design is to develop a wrapper to shield the effect of AES SubBytes from leaking the sensitive power side-channel information. Strategies like current signature attenuation circuits intend to suppress or kill the cryptographic current contributed by AES to the total current drawn from the power supply. It is understandable that in order to overpower the effect of the cryptographic core, the countermeasure has to have a very strong effect on the currents. Low dropout (LDO) regulators are another measure which tend to provide constant voltage regulation at the power supply, so that the current drawn by the cryptographic core appears constant to an attacker. Another endeavor to maintain constant current flowing from the power supply to the cryptographic core is using switched capacitor which stores charge from the supply, then provides charge to the encryption core, and finally discharges to a pre-defined value. These aforementioned countermeasure techniques exhibit constant current at the supply thereby ensuring an attacker is not able to sense the sensitive cryptographic current element in it. Another aspect of dealing with the adversaries is by inserting noise in the AES design itself so that the signal element liberated in the side-channel information is very minimal. Noise insertion can be done by processing false data inside AES using techniques like Secure Double Rate Registers, masking, etc. Such techniques are also very hardware resources demanding, as the countermeasure circuit behavior needs to noisy enough to suppress the AES SubBytes activities.

Having seen the challenges in the countermeasure design techniques, this work initially boosted the intrinsic AES resilience by wisely choosing an S-box, modifying one of the standard mode of operations for its suitability, and splitting the SubBytes to reduce power side-channel information leakage so that only the effect of a single S-box needs to be attended to, by the countermeasure. Eventually, the random number generator using CEB, CCB and LFSRs, assisted with buffer delay blocks are integrated to ensure the power traces are noisy,

Table 6.2: Comparison of the proposed countermeasure w.r.t. state-of-the-art designs.

Countermeasure	Process	Standalone AES power/frequency	Design overheads			MTD	Remarks
			Area	Power	Performance		
Wave dynamic differential logic (WDDL)[188] ♣	180 nm	200 mW @50 MHz, 1.8 V	210%	270%	74.2%	1.2M	Successive stages of the circuit are precharged one after another.
Switched capacitor current equalizer [124] ♣	130 nm	44.34 mW @110 MHz, 1.2 V	7.2%	33%	50%	>10M	Uses capacitors for isolation between encryption core and power supply
Secure double rate registers[94] ♣	65 nm	@20 MHz	33%	180%	0%	>100K	Protection of both combinational and sequential datapaths.
Digital LDO regulator with SNI & V-REF [83] ♣	130 nm	10.9 mW @80 MHz, 0.84 V	36.9%	32%	10.4%	10M	Control-loop induced perturbations in a DLDO.
Heterogeneous S-boxes [186] ♣	14 nm	11 mW @708 MHz, 750 mV	28%	23%	0.7%	12M	Protects the vulnerable attack points of AES.
Non-Linear-DLDO, arithmetic countermeasures [86] ♣	14 nm	-	10%	8%	0.7%	1B	Loop randomizations to improve frequency-domain attack resistance.
Current-domain signature attenuation [145] ♣	65 nm	0.8 mW @50 MHz, 0.8 V	36.7%	49.8%	0%	>1B	Signature suppression of crypto-current in the current domain.
Digital signature attenuation and time-varying transfer function [8] ♣	65 nm	189 μW @ 10 MHz, 0.8 V	28%	33%	0%	>1.25B	Obfuscations in time-domain using a switched capacitor circuit.
Equalizer LDO [151] ♣	65 nm	0.0354 mW @3.3 MHz, 0.45 V	51.85%	1.84%	-	>10M	Protection activated only when device under attack.
Syn-STELLAR [152] ♣	65 nm	0.15 mW @10 MHz, 0.8 V	52%	50%	0%	>1.25B	Analog-based signature attenuation utilized with digital current sources, scalable over technology nodes.
Proposed countermeasure ♠	65 nm	85.289 μW @16 MHz, 1.08 V	-2.91%	-5.61%	-58.61 %	>1M[$]	Expansion and compression-based, assisted with buffer delays.

♣chip-based results ♠simulation-based results [$]on SASEBO

as well as S-box activities operate away from the clock edges. The designed protected AES inclusive of intrinsic and extrinsic security measures contributing to countermeasure action, is compared with state-of-the-art techniques, as shown in Table 6.1, in terms of area, power and performance. It is clearly evident that the proposed design incurs very less area and draws minimal power, as compared to the state-of-the-art designs, however a slight compromise is made on performance. However, the overall achieved throughput of the system is 1.754 Gbps which is sufficient for modern day IoT applications, such as, Bluetooth, RFID, Zigbee, WiFi, 3GPP standards, non 3GPP standards, which work at a throughput level of Mbps. The comparison of the protected design with the state-of-the-art for overheads comparison is presented in Table 6.2. The most striking feature of this countermeasure is that apart from showing resilience to 1 million plaintexts pertaining to CPA attacks, it has a negative area and power overhead. The reference used as an unprotected design, to compare the proposed countermeasure design is the AES with LUT-based S-box in Table 3.1, consuming 23,588.28 μm^2 area, 90.364 μW of power, and a throughput of 3.769 Gbps. Nevertheless, the power consumed by the proposed countermeasure is 85.289 μW which stands least in the standalone AES power column in the table. Owing to the usage of 82-clock strategy, throughput is a compromise, however with IoT applications not demanding a very high speed, this countermeasure befits serving them. Despite the loss in performance, the overall throughput of the proposed design is 1.734 Gbps which very well serves the purpose of IoT standards, such as, Bluetooth, RFID, Zigbee, WiFi, 3GPP standards, non 3GPP standards, in the range of Mbps. Not a single key byte is seen to be cracked using this countermeasure technique even after application of 1 million plaintexts. The most remarkable conclusion from the comparative analysis is that the proposed countermeasure incurs negative area and power overheads compared to the reference design. This is because of the repeated usage of a single S-box to fulfil the AES SubBytes functionality. In addition to the hardware resources advantage, utilizing a single S-box also resulted in minimal leakage of side-channel information owing to which a huge resilience towards CPA was attained.

6.6 Chapter summary

This thesis chapter basically showcases the ultimate AES design incorporating all the intrinsic countermeasure effects discussed in the previous chapters, and adds a small-size physical countermeasure in the form of an expansion-cum-compression circuit. It enlarges the bit size from 8 to 32 and then downsizes it back to 8, with randomization effects produced by LFSR before any expansion or compression. The expansion and compression blocks are also designed with multiplexers to allow concatenated data pass through it. A linear and nonlinear gate component lies between the multiplexers to further enhance the randomization and fail the attacker. With a very intricate countermeasure strategy, both in amplitude-axis as well as time-axis, it is expected to withstand any number of plaintexts during the attacks. The randomization effect is further assisted with buffers delaying the execution of S-boxes, away from the clock edges by a random amount of time decided by the number of 1s in the generated PRNG output. The meaningful samples contributed by the S-box are hence shifted in time domain which fails the basis of CPA attack model requiring perfect alignment of the trace samples contributed by S-boxes. Upon comparison of the proposed countermeasure with state-of-the-art designs, it is found to excel in terms of the overheads, as the design exhibits a negative overhead in terms of area and power. The major reason contributing to the negative overhead is the usage of a single S-box instead of the conventional 16 S-boxes.

CHAPTER

7

CONCLUSION AND FUTURE DIRECTIONS

This thesis initially investigated the intrinsic aspects of amplifying AES' resilience towards PAAs, and transitioned to the incorporation of a small physical countermeasure with negative area and power overheads. With S-Boxes being the heart of the algorithm, the first work was to choose one of its kind which would occupy less area, consume less power and offer a good security. Masoleh S-box was the answer to this investigation which fared better than CMT, Canright and Maximov S-boxes. The conclusion from this work was that owing to lesser gate count and lesser linear gates (which form the basis of the CPA attack model), Masoleh S-box depicted better security results. The next set of work was to investigate the NIST-defined AES' modes of operation, namely, ECB, CBC, CFB, OFB and CTR. Owing to their parallellization of the architecture to process data faster, it demanded a large hardware, for which architectures were suggested. With the conventional CPA attack model, it was possible to attack only the ECB and CBC mode, hence a new attack model was proposed which could successfully attack other attack models, as well. Drawing inspiration from the working of CFB mode, a novel CFB-64 mode was designed based on selective choice of bits. This mechanism does not consider 64-bits out of the intermediate ciphertexts, which carry significant information about the cipher key. Hence, a high resilience was observed for this mode. The third work carried out in the thesis involved splitting the all-important SubBytes operation into multiple clock cycles to reduce power side-channel information leaked to the adversaries. The 82-clock and 162-clock AES designs with 8-clock and 16-clock SubBytes design, showed higher resilience to the attacks owing to the lesser number of S-boxes being processed every clock cycle. Ultimately, the two designs were combined in the form of an 82-clock design with a single S-box operating in every clock edge emulating the 162-clock design. Finally, a countermeasure based on expansion and compression of bits was proposed which involved randomization of the intermediate data using LFSRs and passing of the bits through linear and nonlinear gates parallelly to mar the power signature of AES. Also, a buffer block was used to drive the S-box operations away from the clock edge. The final AES design incorporated the initial three intrinsic efforts and the actual physical countermeasure, which resulted in negative area and power overheads. The prime reason for such a result is the reuse of a single S-box instead of the conventional usage of 16 S-boxes.

With a huge potential to impact the upcoming technology, some directional steps for future are listed below:

1. Findings of this thesis can incorporated to secure modern-day RISC-V processors, as they are being employed for embedded systems, such as microcontrollers, IoT devices, and industrial control systems, due to its simplicity, efficiency, and customizable instruction set.

2. Also, the works can be made adaptable to the trending Post Quantum Cryptography (PQC).

3. Another possible direction is to build on such a work to thwart power attacks as well as fault attacks, such that the same countermeasure can serve to be shielding two types of attacks.

4. With designers all across the globe in an endeavor to secure AES, a common platform or framework to evaluate the resilience is an urgent need of the hour. The same can be said about the metrics not being uniform to measure the resilience of different countermeasures.

5. Off late, researchers have tried to detect if an attack is being performed and then securing the AES, rather than directly jumping to AES' security aspects. This opens an widespread direction in the area of sensor design to detect power attacks.

6. With 5G communication being researched vehemently, ciphers for them and their associated countermeasures is also a potent future direction.

7. Finally, some attention can be paid to circuit-level countermeasures for FPGA security, pertaining to cloud applications.

The thesis concludes on the note that hardware security is an area of immense significance today, holding bright promises and challenges in the upcoming years as well. With human lives getting more and more technologically bound, it is expected that the manpower required to nullify the challenges posed by side-channel attackers is also going to rise manifold. This thesis can serve as a good reference for a fresher intending to embark on the path of securing hardware from side-channel attacks.

PUBLICATIONS

Published

1. **T. B. Singha**, B. Sanjana, T. M. Ignatius, R. P. Palathinkal and S. R. Ahamed, "Improvement in Resilience of AES Design With Reconfigured CFB Mode Against Power Attacks," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, doi: 10.1109/TVLSI.2024.3422501.

2. **T. B. Singha**, R. P. Palathinkal and S. R. Ahamed, "Securing AES Designs Against Power Analysis Attacks: A Survey," in *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14332-14356, 15 Aug.15, 2023, doi: 10.1109/JIOT.2023.3265683.

3. V. Padmakumar, T. M. Ignatius, **T. B. Singha**, R. P. Palathinkal and S. R. Ahamed, "Boosting AES Intrinsic Resilience Using Split SubBytes Round Function Against Power Attacks," in *IEEE Embedded Systems Letters*, doi: 10.1109/LES.2024.3420226.

4. **T. B. Singha**, R. P. Palathinkal and S. R. Ahamed, "Implementation of AES Using Composite Field Arithmetic for IoT Applications," 2020 *Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, Guwahati, India, 2020, pp. 115-121, doi: 10.1109/ISEA-ISAP49340.2020.235009

Under review

1. **T. B. Singha**, R. P. Palathinkal and S. R. Ahamed, "Analysis of S-box Hardware Resources to Improve AES Intrinsic Security Against Power Attacks", in *IEEE Embedded Systems Letters* (revision submitted).

Submitted

1. **T. B. Singha**, B. Sanjana, R. P. Palathinkal and S. R. Ahamed, "AES countermeasure design using expansion and compression-based PRNG with buffer-based random delay technique to thwart power analysis attacks" in *IEEE Transactions on Circuits and Systems-I.*

2. **T. B. Singha**, B. Sanjana, Y. M. Reddy, T. S. Thomas, D. Kumar, R. P. Palathinkal and S. R. Ahamed, "Mitigating power attacks: Effective countermeasure design methodology for AES in IoT edge devices" in *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems.*

BIBLIOGRAPHY

[1] M. Gowtham and H. B. Pramod, "Semantic query-featured ensemble learning model for SQL-injection attack detection in IoT-ecosystems," *IEEE Transactions on Reliability*, vol. 71, no. 2, pp. 1057–1074, 2022.

[2] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2091–2121, 2013.

[3] W. He and Z. Mo, "Secure event-triggered consensus control of linear multiagent systems subject to sequential scaling attacks," *IEEE Transactions on Cybernetics*, pp. 1–14, 2021.

[4] I. Ilahi, M. Usama, J. Qadir, M. U. Janjua, A. Al-Fuqaha, D. T. Hoang, and D. Niyato, "Challenges and countermeasures for adversarial attacks on deep reinforcement learning," *IEEE Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 90–109, 2022.

[5] P. Gu, C. Hua, W. Xu, R. Khatoun, Y. Wu, and A. Serhrouchni, "Control channel anti-jamming in vehicular networks via cooperative relay beamforming," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5064–5077, 2020.

[6] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Lightweight ciphers and their side-channel resilience," *IEEE Transactions on Computers*, vol. 69, no. 10, pp. 1434–1448, 2020.

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

[8] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "An EM/Power SCA-resilient AES-256 with synthesizable signature attenuation using digital-friendly current source and RO-bleed-based integrated local feedback and global switched-mode control," in *2021 IEEE International Solid- State Circuits Conference (ISSCC)*, vol. 64, pp. 499–501, 2021.

[9] Y. Huang, S. Bhunia, and P. Mishra, "Scalable test generation for Trojan detection using side-channel analysis," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2746–2760, 2018.

[10] IEEE Computer Society LAN/MAN Standards Committee and others, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11i*, 2007.

[11] LAN/MAN Standards Committee and others, "IEEE Standard for Local and Metropolitan Area Networks Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for LowRate Wireless Personal Area Networks (LR-WPAN), Part 15.4: wireless Medium Access Control (MAC) and physical layer (PHY) specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Computer Society, IEEE Std 802.15.4*, 2003.

[12] Z. Alliance, "ZigBee Specification Version 1.0, DECEMBER 2004."

[13] V. Rijmen and J. Daemen, "Advanced Encryption Standard," *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pp. 19–22, 2001.

[14] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*, pp. 388–397, Springer, 1999.

[15] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*, vol. 31. Springer Science & Business Media, 2008.

[16] M. Avital, I. Levi, O. Keren, and A. Fish, "CMOS based gates for blurring power information," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 7, pp. 1033–1042, 2016.

[17] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 426–442, Springer, 2008.

[18] B. J. Gilbert Goodwill, J. Jaffe, P. Rohatgi, *et al.*, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, pp. 115–136, 2011.

[19] V. Rijmen, "Efficient Implementation of the Rijndael S-box," *Katholieke Universiteit Leuven, Dept. ESAT. Belgium*, 2000.

[20] T.-F. Lin, C.-P. Su, C.-T. Huang, and C.-W. Wu, "A high-throughput low-cost AES cipher chip," in *Proceedings, IEEE Asia-Pacific Conference on ASIC*, pp. 85–88, IEEE, 2002.

[21] A. Rudra, P. K. Dubey, C. S. Jutla, V. Kumar, J. R. Rao, and P. Rohatgi, "Efficient Rijndael encryption implementation with composite field arithmetic," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 171–184, Springer, 2001.

[22] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 239–254, Springer, 2001.

[23] J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES S-Boxes," in *Cryptographers Track at the RSA Conference*, pp. 67–78, Springer, 2002.

[24] C.-C. Lu and S.-Y. Tseng, "Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter," in *Proceedings IEEE International Conference on Application-Specific Systems, Architectures, and Processors*, pp. 277–285, IEEE, 2002.

[25] N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, "A systematic evaluation of compact hardware implementations for the Rijndael S-box," in *Cryptographers Track at the RSA Conference*, pp. 323–333, Springer, 2005.

[26] Canright, David, "A very compact Rijndael S-box," tech. rep., Naval Postgraduate School Monterey, CA Dept. of Mathematics, 2004.

[27] "CMT: Circuit minimization team." `http://www.cs.yale.edu/homes/peralta/CircuitStuff/CMT.html`, 2016.

[28] J. Boyar and R. Peralta, "A new combinational logic minimization technique with applications to cryptology," in *International Symposium on Experimental Algorithms*, pp. 178–189, Springer, 2010.

[29] A. Reyhani-Masoleh, M. Taha, and D. Ashmawy, "Smashing the implementation records of AES S-box," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 298–336, 2018.

[30] R. Ueno, N. Homma, Y. Sugawara, Y. Nogami, and T. Aoki, "Highly efficient GF(2^8) inversion circuit based on redundant GF arithmetic and its application to AES design," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 63–80, Springer, 2015.

[31] J. Jean, A. Moradi, T. Peyrin, and P. Sasdrich, "Bit-sliding: a generic technique for bit-serial implementations of SPN-based primitives," in *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 687–707, Springer, 2017.

[32] A. Reyhani-Masoleh, M. Taha, and D. Ashmawy, "New area record for the AES combined S-box/inverse S-box," in *IEEE 25th Symposium on Computer Arithmetic (ARITH)*, pp. 145–152, IEEE, 2018.

[33] A. Maximov and P. Ekdahl, "New circuit minimization techniques for smaller and faster AES S-Boxes," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 91–125, 2019.

[34] E. Biham, "A fast new DES implementation in software," in *International Workshop on Fast Software Encryption*, pp. 260–272, Springer, 1997.

[35] H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82 Gbits/sec VLSI implementation of the AES Rijndael algorithm," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 51–64, Springer, 2001.

[36] I. Verbauwhede, P. Schaumont, and H. Kuo, "Design and performance testing of a 2.29-GB/s Rijndael processor," *IEEE Journal of Solid-State Circuits*, vol. 38, no. 3, pp. 569–572, 2003.

[37] A. Hodjat, D. D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede, "A 3.84 Gbits/s AES Crypto Coprocessor with Modes of Operation in a 0.18-μm CMOS Technology," in *Proceedings of the 15th ACM Great Lakes symposium on VLSI*, pp. 60–63, 2005.

[38] S.Morioka and A. Satoh, "A 10-Gbps full-AES crypto design with a twisted BDD S-Box architecture," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 7, pp. 686–691, 2004.

[39] R. E. Bryant, "Graph-based algorithms for boolean function manipulation," *Computers, IEEE Transactions on*, vol. 100, pp. 677–691, 1986.

[40] V. Fischer and M. Drutarovskỳ, "Two methods of Rijndael implementation in reconfigurable hardware," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 77–92, Springer, 2001.

[41] A. Hodjat and I. Verbauwhede, "Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors," *IEEE Transactions on Computers*, vol. 55, no. 4, pp. 366–372, 2006.

[42] S. Mathew, F. Sheikh, A. Agarwal, M. Kounavis, S. Hsu, H. Kaul, M. Anders, and R. Krishnamurthy, "53 Gbps native GF($(2^4)^2$) composite-field AES-encrypt/decrypt accelerator for content-protection in 45nm high-performance microprocessors," in *2010 Symposium on VLSI Circuits*, pp. 169–170, IEEE, 2010.

[43] S. K. Mathew, F. Sheikh, M. Kounavis, S. Gueron, A. Agarwal, S. K. Hsu, H. Kaul, M. A. Anders, and R. K. Krishnamurthy, "53 Gbps Native GF($(2^4)^2$) Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 4, pp. 767–776, 2011.

[44] L. Batina, D. Jakobovic, N. Mentens, S. Picek, A. De La Piedra, and D. Sisejkovic, "S-box pipelining using genetic algorithms for high-throughput AES implementations: How fast can we go?," in *International Conference on Cryptology in India*, pp. 322–337, Springer, 2014.

[45] Y. Wang, L. Ni, C.-H. Chang, and H. Yu, "DW-AES: A domain-wall nanowire-based AES for high throughput and energy-efficient data encryption in non-volatile memory," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2426–2440, 2016.

[46] S. Morioka and A. Satoh, "An optimized S-Box circuit architecture for low power AES design," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 172–186, Springer, 2002.

[47] T. Sasao, "AND-EXOR expressions and their optimization," in *Logic synthesis and optimization*, pp. 287–312, Springer, 1993.

[48] G. Bertoni, M. Macchetti, L. Negri, and P. Fragneto, "Power-efficient ASIC synthesis of cryptographic S-boxes," in *Proceedings of the 14th ACM Great Lakes symposium on VLSI*, pp. 277–281, 2004.

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

[50] N. Pramstaller, S. Mangard, S. Dominikus, and J. Wolkerstorfer, "Efficient AES implementations on ASICs and FPGAs," in *International Conference on Advanced Encryption Standard*, pp. 98–112, Springer, 2004.

[51] Z. Liu, Y. Zeng, X. Zou, Y. Han, and Y. Chen, "A high-security and low-power AES S-box full-custom design for wireless sensor network," in *2007 International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 2499–2502, IEEE, 2007.

[52] N. Ahmad and S. R. Hasan, "Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using novel XOR gate," *Integration*, vol. 46, no. 4, pp. 333–344, 2013.

[53] S. Mathew, S. Satpathy, V. Suresh, M. Anders, H. Kaul, A. Agarwal, S. Hsu, G. Chen, and R. Krishnamurthy, "340 mV–1.1 V, 289 Gbps/W, 2090-gate nano-AES hardware accelerator with area-optimized encrypt/decrypt GF($(2^4)^2$) polynomials in 22 nm tri-gate CMOS," *IEEE Journal of Solid-State Circuits*, vol. 50, no. 4, pp. 1048–1058, 2015.

[54] X. Zhang and K. K. Parhi, "On the optimum constructions of composite field for the AES algorithm," *IEEE Transactions on circuits and systems II: express briefs*, vol. 53, no. 10, pp. 1153–1157, 2006.

[55] S. Morioka and A. Satoh, "A 10 Gbps full-AES crypto design with a twisted-BDD S-Box architecture," in *Proceedings, IEEE International Conference on Computer Design*, pp. 98–103, 2002.

[56] A. Hodjat and I. Verbauwhede, "Minimum area cost for a 30 to 70 Gbits/s AES processor," in *IEEE Computer Society Annual Symposium on VLSI*, pp. 83–88, IEEE, 2004.

[57] P. Hamalainen, T. Alho, M. Hannikainen, and T. D. Hamalainen, "Design and implementation of low-area and low-power AES encryption hardware core," in *9th EUROMICRO conference on digital system design (DSD'06)*, pp. 577–583, IEEE, 2006.

[58] S. B. Ors and B. Preneel, "Power analysis of an FPGA implementation of Rijndael: Is pipelining a dpa countermeasure?," in *in Cryptographic Hardware and Embedded Systems*, Citeseer, 2004.

[59] M. Bucci, R. Luzzi, M. Guglielmo, and A. Trifiletti, "A countermeasure against differential power analysis based on random delay insertion," in *2005 IEEE International Symposium on Circuits and Systems*, pp. 3547–3550, IEEE, 2005.

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

[61] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 169–179, 2014.

[62] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Proceedings of the 52nd Annual Design Automation Conference*, pp. 1–6, 2015.

[63] W. Yu and S. Köse, "Time-delayed converter-reshuffling: An efficient and secure power delivery architecture," *IEEE Embedded Systems Letters*, vol. 7, no. 3, pp. 73–76, 2015.

[64] W. Yu and S. Kse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 5, pp. 438–442, 2016.

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

[66] M. Tunstall and O. Benoit, "Efficient use of random delays in embedded software," in *IFIP International Workshop on Information Security Theory and Practices*, pp. 27–38, Springer, 2007.

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

[68] J. S. Coron and I. Kizhvatov, "Analysis and improvement of the random delay countermeasure of CHES 2009," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 95–109, Springer, 2010.

[69] P. C. Liu, H. C. Chang, and C. Y. Lee, "A low overhead DPA countermeasure circuit based on ring oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 7, pp. 546–550, 2010.

[70] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A true random-based differential power analysis countermeasure circuit for an AES engine," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 59, no. 2, pp. 103–107, 2012.

[71] P.-C. Liu, J.-H. Hsiao, H.-C. Chang, and C.-Y. Lee, "A 2.97 Gb/s DPA-resistant AES engine with self-generated random sequence," in *2011 Proceedings of the ESSCIRC (ESSCIRC)*, pp. 71–74, 2011.

[72] H. Nassar, S. Pankner, L. Bauer, and J. Henkel, "Late breaking results: Configurable ring oscillators as a side-channel countermeasure," in *2023 60th ACM/IEEE Design Automation Conference (DAC)*, pp. 1–2, IEEE, 2023.

[73] X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, "Role of power grid in side channel attack and power-grid-aware secure design," in *Proceedings of the 50th Annual Design Automation Conference*, pp. 1–9, 2013.

[74] A. Kaizerman, S. Fisher, and A. Fish, "Subthreshold dual mode logic," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 5, pp. 979–983, 2013.

[75] M. Avital and A. Fish, "Secured dual mode logic (DML) as a countermeasure against differential power analysis," in *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 810–813, 2014.

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

[77] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *Proceedings of the 2016 International Symposium on Low Power Electronics and Design*, pp. 130–135, 2016.

[78] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved Power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, 2019.

[79] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, 2018.

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

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

[82] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "A 128-b 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)*, pp. 404–406, 2019.

[83] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, 2020.

[84] T. Singh, S. Rangarajan, D. John, C. Henrion, S. Southard, H. McIntyre, A. Novak, S. Kosonocky, R. Jotwani, A. Schaefer, E. Chang, J. Bell, and M. Co, "3.2 Zen: A next-generation high-performance × 86 core," in *2017 IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 52–53, 2017.

[85] Z. Toprak-Deniz, M. Sperling, J. Bulzacchelli, G. Still, R. Kruse, S. Kim, D. Boerstler, T. Gloekler, R. Robertazzi, K. Stawiasz, T. Diemoz, G. English, D. Hui, P. Muench, and J. Friedrich, "Distributed system of digitally controlled microregulators enabling per-core DVFS for the POWER8^{TM} microprocessor," in *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 98–99, 2014.

[86] R. Kumar, X. Liu, V. Suresh, H. K. Krishnamurthy, S. Satpathy, M. A. Anders, H. Kaul, K. Ravichandran, V. De, and S. K. Mathew, "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4k crypto-processor in 14-nm CMOS," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 4, pp. 1141–1151, 2021.

[87] M. Masoumi and M. H. Rezayati, "Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 256–265, 2015.

[88] A. Pradeep, V. Mohanty, A. M. Subramaniam, and C. Rebeiro, "Revisiting AES S-Box Composite Field Implementations for FPGAs," *IEEE Embedded Systems Letters*, vol. 11, no. 3, pp. 85–88, 2019.

[89] M. Avital, H. Dagan, O. Keren, and A. Fish, "Randomized multitopology logic against differential power analysis," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 4, pp. 702–711, 2015.

[90] W. Shan, X. Fu, and Z. Xu, "A secure reconfigurable crypto IC with countermeasures against SPA, DPA, and EMA," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 7, pp. 1201–1205, 2015.

[91] I. Levi, O. Keren, and A. Fish, "Data-dependent delays as a barrier against power attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 8, pp. 2069–2078, 2015.

[92] I. Levi, A. Fish, and O. Keren, "CPA secured data-dependent delay-assignment methodology," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 2, pp. 608–620, 2017.

[93] W. Yu and S. Kse, "Implications of noise insertion mechanisms of different countermeasures against side-channel attacks," in *IEEE International Symposium on Circuits and Systems*, pp. 1–4, 2017.

[94] D. Bellizia, S. Bongiovanni, P. Monsurr, G. Scotti, A. Trifiletti, and F. B. Trotta, "Secure double rate registers as an RTL countermeasure against power analysis attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 7, pp. 1368–1376, 2018.

[95] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 10, pp. 3300–3311, 2018.

[96] I. Levi, A. Fish, and O. Keren, "Low-cost pseudoasynchronous circuit design style with reduced exploitable side information," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 1, pp. 82–95, 2018.

[97] S. N. Dhanuskodi and D. Holcomb, "Enabling microarchitectural randomization in serialized AES implementations to mitigate side channel susceptibility," in *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 314–319, 2019.

[98] S. N. Dhanuskodi, S. Allen, and D. E. Holcomb, "Efficient register renaming architectures for 8-bit AES datapath at 0.55 pj/bit in 16-nm FinFET," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 8, pp. 1807–1820, 2020.

[99] 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)*, pp. 854–862, 2007.

[100] F. Gurkaynak, S. Oetiker, H. Kaeslin, N. Felber, and W. Fichtner, "Improving DPA security by using globally-asynchronous locally-synchronous systems," in *Proceedings of the 31st European Solid-State Circuits Conference, 2005. ESSCIRC 2005.*, pp. 407–410, 2005.

[101] J. Yang, J. Han, F. Dai, W. Wang, and X. Zeng, "A power analysis attack resistant multicore platform with effective randomization techniques," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 6, pp. 1423–1434, 2020.

[102] M. Masoumi, "Novel hybrid CMOS/Memristor implementation of the AES algorithm robust against differential power analysis attack," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 7, pp. 1314–1318, 2020.

[103] P. Sasdrich and T. Gneysu, "A grain in the silicon: SCA-protected AES in less than 30 slices," in *2016 IEEE 27th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pp. 25–32, 2016.

[104] S. Patranabis, D. B. Roy, P. K. Vadnala, D. Mukhopadhyay, and S. Ghosh, "Shuffling across rounds: A lightweight strategy to counter side-channel attacks," in *2016 IEEE 34th International Conference on Computer Design (ICCD)*, pp. 440–443, 2016.

[105] G. Harcha, V. Laptre, C. Chavet, and P. Coussy, "Toward secured IoT devices: A shuffled 8-bit AES hardware implementation," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–4, 2020.

[106] J. Zhou, E. Elgendy, E. Y. Tawfik, and X. Zhang, "Low-complexity aes architectures resilient to power analysis attacks," in *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 165–169, IEEE, 2022.

[107] A. Ghosh, M. A. Rahman, D. Das, S. Ghosh, and S. Sen, "Power and EM SCA resilience in 65nm AES-256 exploiting clock-slew dependent variability in CMOS digital circuits," in *2023 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–2, IEEE, 2023.

[108] M. Brisfors, M. Moraitis, and E. Dubrova, "Do not rely on clock randomization: A side-channel attack on a protected hardware implementation of aes," in *International Symposium on Foundations and Practice of Security*, pp. 38–53, Springer, 2022.

[109] M. Moraitis, M. Brisfors, E. Dubrova, N. Lindskog, and H. Englund, "A side-channel resistant implementation of AES combining clock randomization with duplication," in *2023 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, IEEE, 2023.

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

[111] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 1, pp. 246–251 Vol.1, 2004.

[112] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuits," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 282–297, Springer, 2004.

[113] S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, and J. Provost, "CMOS structures suitable for secured hardware," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 2, pp. 1414–1415 Vol.2, 2004.

[114] D. Suzuki, M. Saeki, and T. Ichikawa, "Random switching logic: A countermeasure against DPA based on transition probability," *Cryptology ePrint Archive*, 2004.

[115] M. Saeki, D. Suzuki, K. Shimizu, and A. Satoh, "A design methodology for a DPA-resistant cryptographic LSI with RSL techniques," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 189–204, Springer, 2009.

[116] D. M. Chapiro, "Globally-asynchronous locally-synchronous systems.," tech. rep., Stanford Univ CA Dept of Computer Science, 1984.

[117] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 232–241, Springer, 2006.

[118] K. J. Kulikowski, V. Venkataraman, Z. Wang, A. Taubin, and M. Karpovsky, "Asynchronous balanced gates tolerant to interconnect variability," in *2008 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 3190–3193, 2008.

[119] T. Akishita, M. Katagi, Y. Miyato, A. Mizuno, and K. Shibutani, "A practical DPA countermeasure with BDD architecture," in *International Conference on Smart Card Research and Advanced Applications*, pp. 206–217, Springer, 2008.

[120] M. Khatir and A. Moradi, "Secure adiabatic logic: A low-energy DPA-resistant logic style," *Cryptology ePrint Archive*, 2008.

[121] C. Monteiro, "A comparison of cellular multiplier cell using secure adiabatic logics," in *Proc. of Int. Conf. Circuit/System, Computers and Communications (ITC-CSCC'12), Sapporo, Japan, July 14-18*, 2012.

[122] C. Monteiro, Y. Takahashi, and T. Sekine, "Low power secure AES S-box using adiabatic logic circuit," in *2013 IEEE Faible Tension Faible Consommation*, pp. 1–4, 2013.

[123] 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*, pp. 64–65,65a, 2009.

[124] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2010.

[125] C. Teegarden, M. Bhargava, and K. Mai, "Side-channel attack resistant ROM-based AES S-box," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 124–129, 2010.

[126] M. Renauld, D. Kamel, F.-X. Standaert, and D. Flandre, "Information theoretic and security analysis of a 65-nanometer DDSLL AES S-box," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 223–239, Springer, 2011.

[127] I. Hassoune, F. Macé, D. Flandre, and J.-D. Legat, "Dynamic differential self-timed logic families for robust and low-power security ICs," *Integration*, vol. 40, no. 3, pp. 355–364, 2007.

[128] M. Yamashina and H. Yamada, "An MOS current mode logic (MCML) circuit for low-power sub-GHz processors," *IEICE Transactions on Electronics*, vol. 75, no. 10, pp. 1181–1187, 1992.

[129] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, "Power-gated MOS current mode logic (PG-MCML): A power aware DPA-resistant standard cell library," in *2011 48th ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1014–1019, IEEE, 2011.

[130] S. Badel, E. Güleyüpolu, Ö. Inaç, A. P. Martinez, P. Vietti, F. K. Gürkaynak, and Y. Leblebici, "A generic standard cell design methodology for differential circuit styles," in *Proceedings of the conference on Design, automation and test in Europe*, pp. 843–848, 2008.

[131] M. Doulcier-Verdier, J.-M. Dutertre, J. Fournier, J.-B. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant AES circuit working on duplicated complemented values," in *2011 IEEE International Solid-State Circuits Conference*, pp. 274–276, 2011.

[132] R. Mayer-Sommer, "Smartly analyzing the simplicity and the power of simple power analysis on smartcards," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 78–92, Springer, 2000.

[133] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 7, pp. 1147–1153, 2011.

[134] S. Bongiovanni, F. Centurelli, G. Scotti, and A. Trifiletti, "Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks," *Journal of Cryptographic Engineering*, vol. 5, no. 4, pp. 269–288, 2015.

[135] M. Allam and M. Elmasry, "Dynamic current mode logic (DYCML): a new low-power high-performance logic style," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 3, pp. 550–558, 2001.

[136] F. Macé, F.-X. Standaert, I. Hassoune, J.-D. Legat, J.-J. Quisquater, *et al.*, "A dynamic current mode logic to counteract power analysis attacks," in *Proc. 19th International Conference on Design of Circuits and Integrated Systems (DCIS)*, pp. 186–191, 2004.

[137] H. Kim, V. Rozic, and I. Verbauwhede, "Three phase dynamic current mode logic: a more secure DyCML to achieve a more balanced power consumption," in *International Workshop on Information Security Applications*, pp. 68–81, Springer, 2012.

[138] X. Li, C. Yang, J. Ma, Y. Liu, and S. Yin, "Energy-efficient side-channel attack countermeasure with awareness and hybrid configuration based on it," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3355–3368, 2017.

[139] 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)*, pp. C246–C247, 2015.

[140] W.-H. Ma, J. C. Kao, V. S. Sathe, and M. Papaefthymiou, "A 187MHz subthreshold-supply robust FIR filter with charge-recovery logic," in *2009 Symposium on VLSI Circuits*, pp. 202–203, 2009.

[141] W. Shan, S. Zhang, J. Xu, M. Lu, L. Shi, and J. Yang, "Machine learning assisted side-channel-attack countermeasure and its application on a 28-nm AES circuit," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 3, pp. 794–804, 2020.

[142] S. Lu, Z. Zhang, and M. Papaefthymiou, "A 1.25pJ/bit 0.048mm^2 AES core with DPA resistance for IoT devices," in *2017 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, pp. 65–68, 2017.

[143] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 62–67, 2017.

[144] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D. Seo, M. Chang, A. Varna, H. Krishnamurthy, S. Mathew, S. Ghosh, A. Raychowdhury, and S. Sen, "EM and Power SCA-resilient AES-256 in 65nm CMOS through >350× current-domain signature attenuation," in *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pp. 424–426, 2020.

[145] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D.-H. Seo, M. Chang, A. L. Varna, H. K. Krishnamurthy, S. Mathew, S. Ghosh, A. Raychowdhury, and S. Sen, "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," *IEEE Journal of Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, 2021.

[146] D. Fujimoto, D. Tanaka, N. Miura, M. Nagata, Y.-i. Hayashi, N. Homma, S. Bhasin, and J.-L. Danger, "Side-channel leakage on silicon substrate of CMOS cryptographic chip," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 32–37, 2014.

[147] M. Wang, S. Xie, P. N. Li, A. Sayal, G. Li, V. V. Iyer, A. Thimmaiah, M. Orshansky, A. E. Yilmaz, and J. P. Kulkarni, "Galvanically isolated, power and electromagnetic side-channel attack resilient secure AES core with integrated charge pump based power management," in *2021 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 1–2, 2021.

[148] N. Mohan, T. M. Undeland, and W. P. Robbins, *Power electronics: converters, applications, and design*. John wiley & sons, 2003.

[149] Y. He and K. Yang, "A 65nm edge-chasing quantizer-based digital LDO featuring 4.58ps-FoM and side-channel-attack resistance," in *2020 IEEE International Solid-State Circuits Conference - (ISSCC)*, pp. 384–386, 2020.

[150] N. Miura, D. Fujimoto, R. Korenaga, K. Matsuda, and M. Nagata, "An intermittent-driven supply-current equalizer for 11x and 4x power-overhead savings in CPA-resistant 128-bit AES cryptographic processor," in *2014 IEEE Asian Solid-State Circuits Conference (A-SSCC)*, pp. 225–228, 2014.

[151] S. J. Kim, D. Kim, A. Sharma, and M. Seok, "EQZ-LDO: A near-zero EDP overhead, >10m-attack-resilient, secure digital LDO featuring attack-detection and detection-driven protection for a correlation-power-analysis-resilient IoT device," in *2021 Symposium on VLSI Circuits*, pp. 1–2, 2021.

[152] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-stellar: An em/power sca-resilient aes-256 with synthesis-friendly signature attenuation," *IEEE Journal of Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, 2021.

[153] A. Ghosh, D.-H. Seo, D. Das, S. Ghosh, and S. Sen, "A digital cascoded signature attenuation countermeasure with intelligent malicious voltage drop attack detector for em/power sca resilient parallel aes-256," in *2022 IEEE Custom Integrated Circuits Conference (CICC)*, pp. 01–02, IEEE, 2022.

[154] T. S. Messerges, "Securing the AES finalists against power analysis attacks," in *International Workshop on Fast Software Encryption*, pp. 150–164, Springer, 2000.

[155] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 309–318, Springer, 2001.

[156] L. De Meyer, O. Reparaz, and B. Bilgin, "Multiplicative masking for AES in hardware," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 431–468, 2018.

[157] J. D. Golić and C. Tymen, "Multiplicative masking and power analysis of AES," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 198–212, Springer, 2002.

[158] E. Trichina, "Combinational logic design for AES subbyte transformation on masked data," *Cryptology EPrint Archive*, 2003.

[159] J. Blömer, J. Guajardo, and V. Krummel, "Provably secure masking of AES," in *International workshop on selected areas in cryptography*, pp. 69–83, Springer, 2004.

[160] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-box," in *International workshop on fast software encryption*, pp. 413–423, Springer, 2005.

[161] S. Mangard, T. Popp, and B. M. Gammel, "Side-channel leakage of masked CMOS gates," in *Cryptographers Track at the RSA Conference*, pp. 351–365, Springer, 2005.

[162] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully attacking masked AES hardware implementations," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 157–171, Springer, 2005.

[163] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 255–269, Springer, 2006.

[164] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 172–186, Springer, 2005.

[165] S. Nikova, C. Rechberger, and V. Rijmen, "Threshold implementations against side-channel attacks and glitches," in *International conference on information and communications security*, pp. 529–545, Springer, 2006.

[166] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 242–268, Springer, 1984.

[167] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[168] Y. Desmedt, "Some recent research aspects of threshold cryptography," in *International Workshop on Information Security*, pp. 158–173, Springer, 1997.

[169] B. Bilgin, B. Gierlichs, S. Nikova, V. Nikov, and V. Rijmen, "A more efficient AES threshold implementation," in *International Conference on Cryptology in Africa*, pp. 267–284, Springer, 2014.

[170] J. Song, K. Lee, and J. Park, "Low area and low power threshold implementation design technique for aes s-box," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 70, no. 3, pp. 1169–1173, 2022.

[171] Z. Chen and Y. Zhou, "Dual-rail random switching logic: a countermeasure to reduce side channel leakage," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 242–254, Springer, 2006.

[172] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 81–94, Springer, 2007.

[173] A. Moradi, T. Eisenbarth, A. Poschmann, and C. Paar, "Power analysis of single-rail storage elements as used in MDPL," in *International Conference on Information Security and Cryptology*, pp. 146–160, Springer, 2009.

[174] A. Moradi, M. Kirschbaum, T. Eisenbarth, and C. Paar, "Masked dual-rail precharge logic encounters state-of-the-art power analysis methods," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 9, pp. 1578–1589, 2012.

[175] H. Kim, S. Hong, and J. Lim, "A fast and provably secure higher-order masking of AES S-box," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 95–107, Springer, 2011.

[176] L. Goubin and A. Martinelli, "Protecting AES with Shamir's secret sharing scheme," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 79–94, Springer, 2011.

[177] M. Rivain and E. Prouff, "Provably secure higher-order masking of AES," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 413–427, Springer, 2010.

[178] F.-x. Standaert, G. Rouvroy, and J.-j. Quisquater, "FPGA implementations of the DES and triple-DES masked against power analysis attacks," in *2006 International Conference on Field Programmable Logic and Applications*, pp. 1–4, 2006.

[179] F. Regazzoni, Y. Wang, F.-X. Standaert, *et al.*, "FPGA implementations of the AES masked against power analysis attacks," *Proceedings of COSADE*, vol. 2011, pp. 56–66, 2011.

[180] E. Prouff and M. Rivain, "A generic method for secure S-box implementation," in *International Workshop on Information Security Applications*, pp. 227–244, Springer, 2007.

[181] M. Nassar, Y. Souissi, S. Guilley, and J.-L. Danger, "RSM: A small and fast countermeasure for AES, secure against 1^{st} and 2^{nd}-order zero-offset SCAs," in *2012 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 1173–1178, 2012.

[182] Y. Wang and Y. Ha, "FPGA-based 40.9-Gbits/s masked AES with area optimization for storage area network," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 60, no. 1, pp. 36–40, 2013.

[183] J. Balasch, B. Gierlichs, O. Reparaz, and I. Verbauwhede, "DPA, bitslicing and masking at 1 GHz," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 599–619, Springer, 2015.

[184] W. Yu and S. Kse, "A lightweight masked AES implementation for securing IoT against CPA attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 11, pp. 2934–2944, 2017.

[185] R. Kumar, V. Suresh, M. Kar, S. Satpathy, M. Anders, H. Kaul, A. Agarwal, S. Hsu, G. Chen, R. Krishnamurthy, V. De, and S. Mathew, "A 4900μm^2 839Mbps side-channel attack resistant AES-128 in 14nm CMOS with heterogeneous S-boxes, linear masked mixcolumns and dual-rail key addition," in *2019 Symposium on VLSI Circuits*, pp. C234–C235, 2019.

[186] R. Kumar, V. Suresh, M. Kar, S. Satpathy, M. A. Anders, H. Kaul, A. Agarwal, S. Hsu, G. K. Chen, R. K. Krishnamurthy, V. De, and S. K. Mathew, "A 4900- μm^2 839-Mb/s side-channel attack-resistant AES-128 in 14-nm CMOS with heterogeneous S-boxes, linear masked mixcolumns, and dual-rail key addition," *IEEE Journal of Solid-State Circuits*, vol. 55, no. 4, pp. 945–955, 2020.

[187] R. Kumar, V. B. Suresh, S. Taneja, M. A. Anders, S. Hsu, A. Agarwal, V. De, and S. K. Mathew, "A 7-gbps sca-resistant multiplicative-masked aes engine in intel 4 cmos," *IEEE Journal of Solid-State Circuits*, vol. 58, no. 4, pp. 1106–1116, 2022.

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

[189] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: A very compact and a threshold implementation of AES," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 69–88, Springer, 2011.

[190] T. B. Singha, R. P. Palathinkal, and S. R. Ahamed, "Securing AES designs against power analysis attacks: A survey," *IEEE Internet of Things Journal*, pp. 1–1, 2023.

[191] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, *Applications of finite fields*, vol. 199. Springer Science & Business Media, 2013.

[192] A. Reyhani-Masoleh, M. Taha, and D. Ashmawy, "New low-area designs for the AES forward, inverse and combined s-boxes," *IEEE Transactions on Computers*, vol. 69, no. 12, pp. 1757–1773, 2019.

[193] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 549–562, Springer, 1990.

[194] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE International Solid-State Circuits Conference-Digest of Technical Papers*, pp. 64–65, 2009.

[195] M. Dworkin, "Recommendation for block cipher modes of operation. methods and techniques," tech. rep., National Inst of Standards and Technology Gaithersburg MD Computer security Div, 2001.

[196] A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 9, no. 4, pp. 545–557, 2001.

[197] F. Charot, E. Yahya, and C. Wagner, "Efficient modular-pipelined AES implementation in counter mode on Altera FPGA," in *Field Programmable Logic and Application: 13th International Conference, FPL 2003, Lisbon, Portugal, September 1-3, 2003 Proceedings 13*, pp. 282–291, Springer, 2003.

[198] M. McLoone and J. V. McCanny, "High performance single-chip FPGA Rijndael algorithm implementations," in *Cryptographic Hardware and Embedded SystemsCHES 2001: Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3*, pp. 65–76, Springer, 2001.

[199] M. Xie, S. Li, A. O. Glova, J. Hu, and Y. Xie, "Securing emerging nonvolatile main memory with fast and energy-efficient AES in-memory implementation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 26, no. 11, pp. 2443–2455, 2018.

[200] S. Mangard, M. Aigner, and S. Dominikus, "A highly regular and scalable AES hardware architecture," *IEEE Transactions on Computers*, vol. 52, no. 4, pp. 483–491, 2003.

[201] M. Alam, S. Ray, D. Mukhopadhayay, S. Ghosh, D. RoyChowdhury, and I. Sengupta, "An area optimized reconfigurable encryptor for AES-Rijndael," in *2007 Design, Automation & Test in Europe Conference & Exhibition*, pp. 1–6, IEEE, 2007.

[202] V.-P. Hoang, V.-L. Dao, C.-K. Pham, *et al.*, "A compact, ultra-low power AES-CCM IP core for wireless body area networks," in *2016 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, pp. 1–4, IEEE, 2016.

[203] R. Ueno, S. Morioka, N. Homma, and T. Aoki, "A high throughput/gate AES hardware architecture by compressing encryption and decryption datapaths: toward efficient CBC-mode implementation," in *Cryptographic Hardware and Embedded Systems–CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings 18*, pp. 538–558, Springer, 2016.

[204] J. Jaffe, "A first-order DPA attack against AES in counter mode with unknown initial counter," in *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*, pp. 1–13, Springer, 2007.

[205] M. Taha and P. Schaumont, "Key updating for leakage resiliency with application to AES modes of operation," *IEEE transactions on information forensics and security*, vol. 10, no. 3, pp. 519–528, 2014.

[206] R. Ueno, S. Morioka, N. Miura, K. Matsuda, M. Nagata, S. Bhasin, Y. Mathieu, T. Graba, J.-L. Danger, and N. Homma, "High throughput/gate aes hardware architectures based on datapath compression," *IEEE Transactions on Computers*, vol. 69, no. 4, pp. 534–548, 2019.

[207] A. A. Pammu, W.-G. Ho, N. K. Z. Lwin, K.-S. Chong, and B.-H. Gwee, "A high throughput and secure authentication-encryption aes-ccm algorithm on asynchronous multicore processor," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1023–1036, 2018.

[208] F. Kenarangi and I. Partin-Vaisband, "Exploiting machine learning against on-chip power analysis attacks: Tradeoffs and design considerations," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 2, pp. 769–781, 2018.