2018

# ENERGY-EFFICIENT AND SECURE HARDWARE FOR INTERNET OF THINGS (IoT) DEVICES

Dinesh Kumar Selvakumaran
*University of Kentucky*, dinesh.iiitdm@gmail.com
Digital Object Identifier: https://doi.org/10.13023/etd.2018.510

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Dinesh Kumar Selvakumaran, Student

Dr. Himanshu Thapliyal, Major Professor

Dr. Aaron Cramer, Director of Graduate Studies

# ENERGY-EFFICIENT AND SECURE HARDWARE FOR INTERNET OF THINGS (IoT) DEVICES

---

DISSERTATION

---

A dissertation submitted in partial fulfillment of the
requirements for the degree of Doctor of Philosophy
in the College of Engineering at the
University of Kentucky

By
Dinesh Kumar Selvakumaran
Lexington, Kentucky

Director: Dr. Himanshu Thapliyal, Assistant Professor of
Electrical and Computer Engineering
Lexington, Kentucky
2018

**ABSTRACT OF DISSERTATION**

ENERGY-EFFICIENT AND SECURE HARDWARE FOR INTERNET OF THINGS (IoT) DEVICES

Internet of Things (IoT) is a network of devices that are connected through the Internet to exchange the data for intelligent applications. Though IoT devices provide several advantages to improve the quality of life, they also present challenges related to security. The security issues related to IoT devices include leakage of information through Differential Power Analysis (DPA) based side channel attacks, authentication, piracy, etc. DPA is a type of side-channel attack where the attacker monitors the power consumption of the device to guess the secret key stored in it. There are several countermeasures to overcome DPA attacks. However, most of the existing countermeasures consume high power which makes them not suitable to implement in power constraint devices. IoT devices are battery operated, hence it is important to investigate the methods to design energy-efficient and secure IoT devices not susceptible to DPA attacks. In this research, we have explored the usefulness of a novel computing platform called adiabatic logic, low-leakage FinFET devices and Magnetic Tunnel Junction (MTJ) Logic-in-Memory (LiM) architecture to design energy-efficient and DPA secure hardware. Further, we have also explored the usefulness of adiabatic logic in the design of energy-efficient and reliable Physically Unclonable Function (PUF) circuits to overcome the authentication and piracy issues in IoT devices.

Adiabatic logic is a low-power circuit design technique to design energy-efficient hardware. Adiabatic logic has reduced dynamic switching energy loss due to the recycling of charge to the power clock. As the first contribution of this dissertation, we have proposed a novel DPA-resistant adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL). EE-SPFAL based circuits are energy-efficient compared to the conventional CMOS based design because of recycling the charge after every clock cycle. Further, EE-SPFAL based circuits consume uniform power irrespective of input data transition which makes them resilience against DPA attacks.

Scaling of CMOS transistors have served the industry for more than 50 years in providing integrated circuits that are denser, and cheaper along with its high performance, and low power. However, scaling of the transistors leads to increase in leakage current. Increase in leakage current reduces the energy-efficiency of the computing circuits,and increases their vulnerability to DPA attack. Hence, it is important to investigate the crypto circuits in low leakage devices such as FinFET to make them energy-efficient and DPA resistant. In this dissertation, we have proposed a novel FinFET based Secure Adiabatic Logic (FinSAL) family. FinSAL based designs utilize the low-leakage FinFET device along with adiabatic logic principles to improve energy-efficiency along with its resistance against DPA attack.

Recently, Magnetic Tunnel Junction (MTJ)/CMOS based Logic-in-Memory (LiM) circuits have been explored to design low-power non-volatile hardware. Some of the advantages of MTJ device include non-volatility, near-zero leakage power, high integration density and easy compatibility with CMOS devices. However, the differences in power consumption between the switching of MTJ devices increase the vulnerability of Differential Power Analysis (DPA) based side-channel attack. Further, the MTJ/CMOS hybrid logic circuits which require frequent switching of MTJs are not very energy-efficient due to the significant energy required to switch the MTJ devices. In the third contribution of this dissertation, we have investigated a novel approach of building cryptographic hardware in MTJ/CMOS circuits using Look-Up Table (LUT) based method where the data stored in MTJs are constant during the entire encryption/decryption operation.

Currently, high supply voltage is required in both writing and sensing operations of hybrid MTJ/CMOS based LiM circuits which consumes a considerable amount of energy. In order to meet the power budget in low-power devices, it is important to investigate the novel design techniques to design ultra-low-power MTJ/CMOS circuits. In the fourth contribution of this dissertation, we have proposed a novel energy-efficient Secure MTJ/CMOS Logic (SMCL) family. The proposed SMCL logic family consumes uniform power irrespective of data transition in MTJ and more energy-efficient compared to the state-of-art MTJ/ CMOS designs by using charge sharing technique.

The other important contribution of this dissertation is the design of reliable Physical Unclonable Function (PUF). Physically Unclonable Function (PUF) are circuits which are used to generate secret keys to avoid the piracy and device authentication problems. However, existing PUFs consume high power and they suffer from the problem of generating unreliable bits. This dissertation have addressed this issue in PUFs by designing a novel adiabatic logic based PUF. The time ramp voltages in adiabatic PUF is utilized to improve the reliability of the PUF along with its energy-efficiency. Reliability of the adiabatic logic based PUF proposed in this dissertation is tested through simulation based temperature variations and supply voltage variations.

**KEYWORDS:** Low power, DPA, adiabatic logic, hybrid MTJ/CMOS, PUF.

Dinesh Selvakumaran

November $2^{nd}$, 2018

# ENERGY-EFFICIENT AND SECURE HARDWARE FOR INTERNET OF THINGS (IOT) DEVICES

By

Dinesh Kumar Selvakumaran

Dr. Himanshu Thapliyal

Director of Dissertation

Dr. Aaron Cramer

Director of Graduate Studies

November $2^{nd}$, 2018

Date

# ACKNOWLEDGEMENTS

I like to thank my advisor, Dr. Himanshu Thapliyal, for his continuous guidance, patience and support throughout the course of my doctoral studies. Being a part of VLSI Emerging Design And Nano Things Security (VEDANTS-Lab) helped me to grow as an independent researcher.

I would like to thank Dr. Vijay Singh, Dr. Samson Cheung, and Dr. Dakshinamoorthy Manivannan for taking their time to be a part of my PhD dissertation committee and providing valuable suggestions to improve this dissertation. I also like to thank Dr. Abhijit Patwardhan for serving as an external examiner during my PhD dissertation. I am extremely grateful to Dr. Noor Mahammad, IIITDM for providing me inspirational thoughts and confidence in me to pursue research. I also like to thank Dr. Binsu Kailath, IIITDM for being an incredible teacher in teaching me VLSI concepts.

My PhD journey would not be as fun or challenging if not for my fellow labmates in VEDANTS lab. I would like to thank Carson Labrado, Azhar Mohammad, Rajdeep Kumar Nath, Varun, Shalom and other lab members for their continuous support and encouragement. I like to thank all my friends in Lexington who has been a part of my life during the wonderful journey of PhD.

I like to thank my parents for their love, support and encouragement to achieve my goals irrespective of the circumstances. I also like to thank all my family, friends and professors in India who has always been a support for all my decisions. Finally, I would like to thank my wife for her wonderful support and understanding during the journey of my PhD.

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

Internet of Things (IoT) is a network of machines, physical objects, people and other devices that are connected through the Internet to exchange the data for intelligent applications [10]. These IoT devices include smart phones, tablets, smart cards, consumer electronics, Radio Frequency Identification (RFID) tags, etc. IoT allows direct integration of physical objects and the digital world to improve the quality and productivity of life. Examples of IoT systems include smart homes, smart health, smart cities, etc. as shown in Figure 1.1. Within the past decade, numerous IoT devices have been introduced in the market. Currently, there are around 15 billion IoT devices in the market [24]. It is expected that over 50 billion IoT devices will be connected with each other, creating as much as US$8.9 trillion in annual revenue by the year 2020 [44]. Mckinsey Global Institute reported that the number of connected IoT devices has grown over 300% between the years 2007 and 2012 [47]. Navigant recently reported that the Building Automation Systems market is expected to rise from $58.1 billion in 2013 to $100.8 billion by 2021 [1]. All these statistics show that there is potential for significant and fast-pace growth in IoT related industries and services.

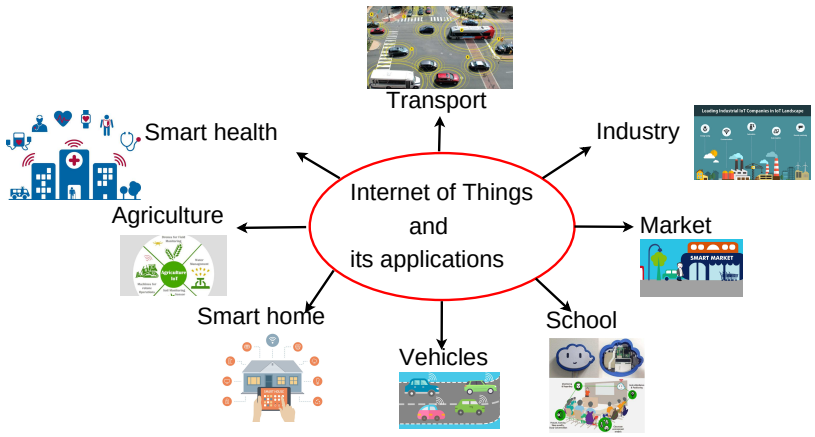



Figure 1.1: Internet of Things (IoT) and its applications.

## 1.1 Challenges in IoT nodes

IoT systems consist of arrays of sensors to gather information from physical sources and offer the means to establish a network connection to transmit the collected information to the remote node. This information can be personal health related information such as heart-beat information, living habits information etc., location of the person or other information such as temperature, humidity etc. [5]. Based on diverse application of IoT nodes, the main design concerns include low-power or low-energy designs and security challenges.

### 1.1.1 Energy constraint

IoT devices are used to sense the phenomena and transfer the information through wired or wireless sources. Unlike the previous computing platforms such as desktop or mobile phones, IoT devices are deployed in places where there is less human interaction. Generally, these devices are deployed in places where there is no easy access to constant power supplies. So, the power or energy required devices are usually battery operated or uses energy harvesters to power themselves. IoT devices or nodes are usually small and battery operated [8]. In other words, IoT devices are resource constrained. IoT devices typically require long lifetimes, further constraining power consumption. Figure 1.2 shows the maximum average power of a device as a function of different batteries and their required

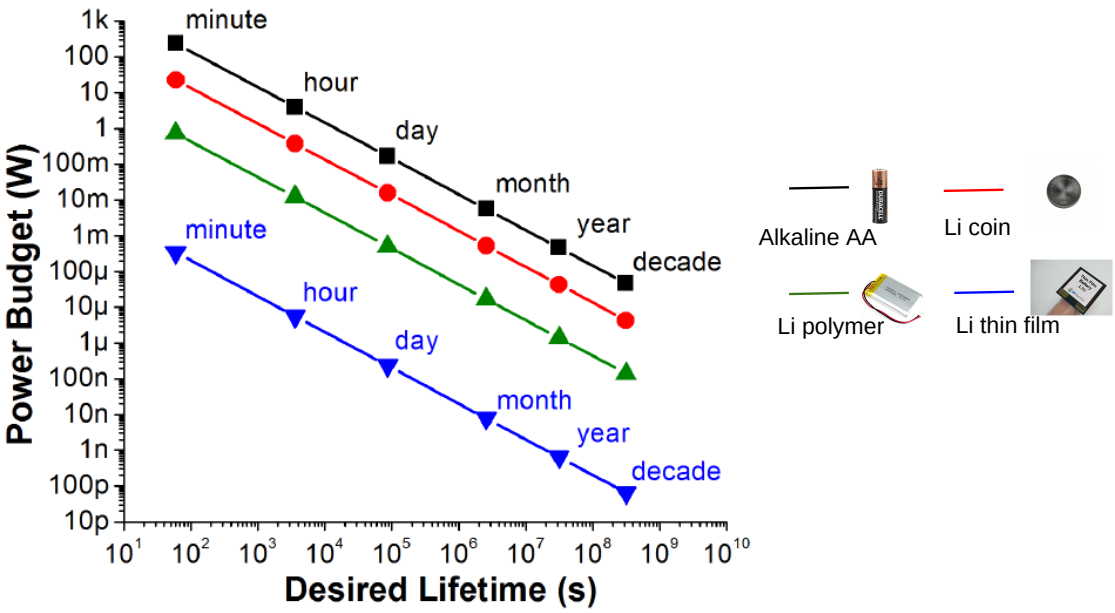



Figure 1.2: Average life time of different batteries Vs power consumption [12].

lifetime [12]. The larger electronic devices with the access to power supply can afford $\mu$W-mW of average power, while the battery operated IoT devices should survive at nW of power budget.

**Technology**

Various novel devices, novel circuit design techniques, etc. have been explored by researchers to address the power budget issue in IoT devices. Among the various device structures, FinFET devices have been widely adopted by industries for the design of low power IoT nodes. For example, Taiwan Semiconductor Manufacturing Limited has launched 16nm FinFET technology for IoT and wearable device applications. Similarly, Intel has developed a new manufacturing process for 22nm FinFET device technologies. Better gate control in FinFETs over MOSFETs results in higher on-state current, lower leakage, and faster switching speed. Further, other nano emerging device based architecture such as non-volatile memory based Logic-in-Memory (LiM) circuits have been explored to design low-power embedded hardware. Among the various non-volatile memory devices,

Spin Transfer Torque Magnetic Tunnel Junction (STT-MTJ) is considered as one of the promising devices for designing low-power non-volatile embedded hardware. Some of the advantages of an STT-MTJ device include non-volatility, near-zero leakage power, high integration density and easy compatibility with CMOS devices [22],[32],[33], [30]. Hybrid MTJ/CMOS based Logic-in-Memory (LiM) architecture show high potential in designing low power embedded hardware [90],[73].

**Circuit design**

Power budget issue in IoT devices can be addressed by employing some of the low-power design methodologies in IoT devices. Some of the well-known methods to reduce power consumption in CMOS based devices are sub-threshold and near-threshold logic. In sub-threshold and near-threshold computations, the logic levels are moved closer to the threshold point of the CMOS transistors, reducing the voltage swing and thereby reducing the power consumption. However, sub-threshold and near-threshold computation are prone to high error rates [84]. Adiabatic logic [7] is another circuit design technique used to design energy-efficient hardware. Adiabatic logic uses power clocks to efficiently recycle the charge stored in the load capacitor. Because of the recycling of charge, adiabatic logic has reduced dynamic switching energy loss. Recently, researchers from Stony Brook University have stated that adiabatic logic or charge recycling circuit can be considered as an alternative computing paradigm to wirelessly power the IoT devices. In adiabatic logic circuits, harvested AC power can be used directly for computation by leveraging the energy recycling theory [82], [81].

### 1.1.2 Security constraint

Along with the energy constraint, security is the other major concern in the design of IoT devices. IoT nodes usually gather and store personal information. The storage of information by the IoT devices makes it a target for attackers to obtain the data. Further, employing

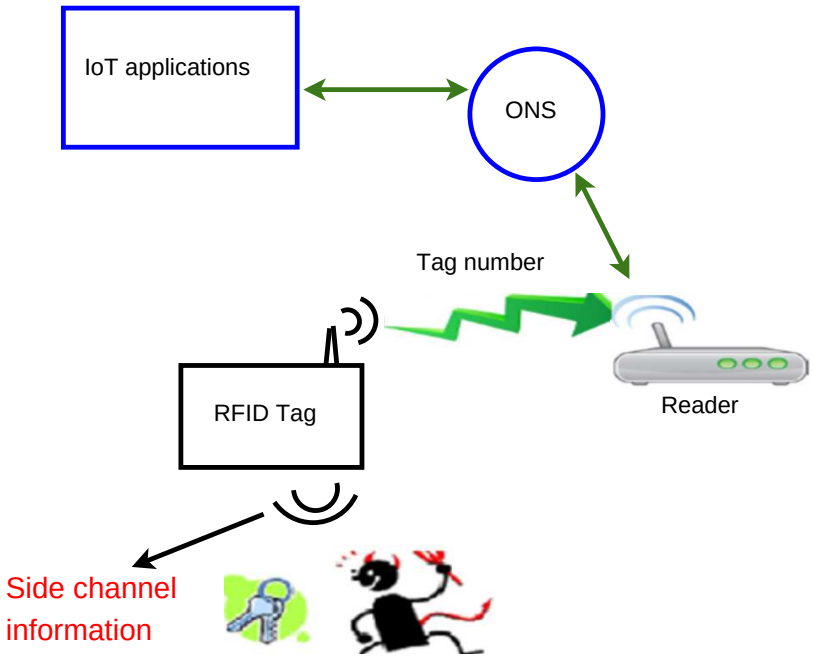



Figure 1.3: Hardware attack scenario in an IoT node using side channel information.

the conventional security mechanisms directly in IoT devices are highly challenging due to their resource constraints. Although IoT device manufacturers are aware of the privacy and security implications in IoT devices, these issues are either neglected or treated as second thought. This is often due to short time to market and reduction of device costs through the design and development process of the device. Few IoT devices that choose to add protection usually employ software level solutions, where the methods resemble those used in regular computing [5]. However, when a device is exposed to hardware based attacks, it will be tough for the manufacturers to update the hardware. So, hardware attack based countermeasures need to be considered during the design process of the device.

### Side channel attacks

There are several kinds of hardware attacks on the IoT device. An IoT device employs cryptographic algorithms to perform encryption/decryption operations. For example, IoT devices such as smart cards, and RFID tags are cryptographic devices which are used to store secret keys and perform cryptographic operations [46]. Hardware attacks can be

broadly classified as invasive attack, semi-invasive attack and non-invasive attack [46]. These attacks are classified based on the interface that is used for the attack.

An invasive attack is a type of attack where the cryptographic device will be depackaged. Further, different components of the device are accessed directly using a special device. These devices include laser cutters, probing stations or focused ion beams. While invasive attacks are powerful, they typically require expensive equipment [66],[46]. In semi-invasive attacks, the cryptographic device is still depackaged. However, in semi-invasive attack, no direct electrical contact to a chip surface is made. The goal of the semi-invasive attack is to read out the content of memory cells without using the normal read out circuits. Semi-invasive attacks do not require expensive equipment. However, the total effort to conduct a semi-invasive attack on a cryptographic device is relatively high. In non-invasive attack, the cryptographic device is attacked without altering the functionality of the device. Most of the non-invasive attacks can be conducted by using inexpensive equipment and hence these attacks pose a serious threat to the cryptographic devices [46]. Passive non-invasive attacks are also referred as side channel analysis attacks.

Side-channel analysis attack is a type of non-invasive attack where the information stored in the cryptographic device is leaked through side channel information. Side-channel attacks include power analysis attacks [35], timing attacks [23], electromagnetic attacks [77], etc. Figure 1.3 shows the hardware attack scenario where the attacker captures the side-channel information from the RFID tag to guess the secret key used to generate the tag number and sends to Object Naming Service (ONS) for performing the desired task. Attacking the IoT node helps to manipulate the data in IoT applications which can lead to severe damage or property loss to the public. Among all the attacks, Differential Power Analysis (DPA) attack [35] is one of the side-channel attack well proven in successfully attacking smart cards or other dedicated embedded systems containing the secret key [49].

Differential Power Analysis (DPA) attack is a type of power analysis attack which exploits the correlation between the instantaneous power consumed by the device and the

processed data and the secret key [9] [35]. In DPA attack, the attackers do not require any information about the actual hardware implementation of the device. Still, the attacker must know which algorithm to attack since the DPA attack requires a known model of cipher behavior.

**Authentication and piracy issue**

Other important security concerns for IoT devices are authentication and piracy [48]. It is expected that there will be more than 50 billion IoT device in the real world market. Further, most of the IoT devices are deployed in remote locations. So, these devices must be equipped with a way to identify and authenticate itself. The second concern for the IoT device is the cloning attack. IoT devices are deployed in open. An attacker may easily access an IoT device and extract the secret keys to clone the device. Currently, the secret keys which are used for authentication are stored in non-volatile memories. However, the secret keys are vulnerable to active attacks [48], [4], [40]. Moreover, implementing a tamper resistant circuitry in IoT devices to provide high level physical security may be very expensive in terms of cost and energy.

## 1.2 Motivation

IoT devices provide several advantages to improve the quality of life. However, they also equally present challenges related to power consumption and security of IoT devices. Improvement in security of IoT devices comes at the cost of reduction in battery life. IoT devices collect the real-world data and connect to the Internet. In doing so, they emit signals known as side channels. Side channel information can be retrieved from an IoT device during the encryption of real world data. Some of the examples of side-channel information include power consumption of IoT device, electromagnetic emission, etc. This “leaked side-channel information” is related to underlying computation or keys, giving clues useful

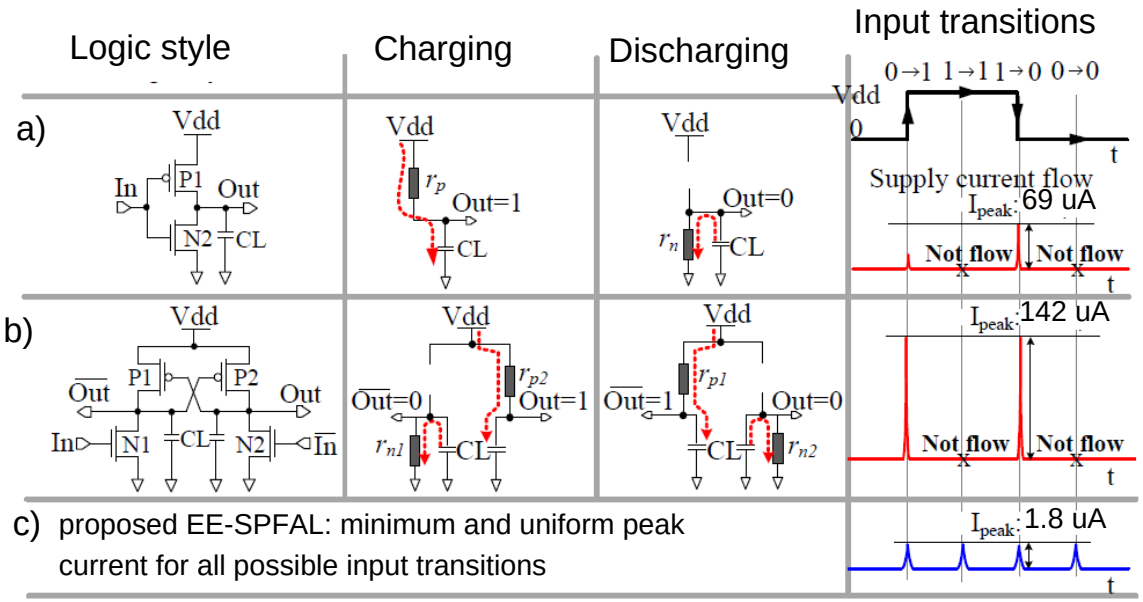



Figure 1.4: Current traces of an inverter implemented using a) conventional CMOS logic, b) Dual rail CMOS family, c) Proposed adiabatic logic based DPA resistant family.

for attackers to perform attacks known as side-channel attacks. Side-channel attacks on IoT devices are of concern as these attacks can be mounted quickly on IoT devices without disturbing its operation. Among the various side-channel attacks, the attack by monitoring the power consumption of IoT device is one of the biggest concerns and is called Differential Power Analysis (DPA) attack. Various DPA countermeasures have been proposed to protect the cryptographic systems [55]. These schemes can be broadly classified as algorithm/architectural techniques [63], [3] and cell level techniques [75], [15]. Algorithm/architecture techniques modify the intermediate computation steps of the algorithms to mask the power consumption of the device. However, this countermeasure technique is unique to each algorithm and does not provide a generic solution. The other countermeasure is utilizing the cell level techniques to counteract the DPA attack. In this method, the supply current is independent of the inputs to the logic gates. Some of the well known DPA resistance circuit family include Sense Amplifier Based Logic (SABL) [74], Wave Dynamic Differential Logic (WDDL) [75], etc. However, existing cell level countermeasures consume more power than the conventional CMOS based circuit which makes them

not suitable to implement in battery operated IoT devices. In a survey of broad range of countermeasures against DPA attack, adiabatic logic based countermeasure is considered as suitable cell level countermeasures to implement DPA resistant hardware.

Figure 1.4 shows the current traces of the inverter implemented using a conventional CMOS logic, a dual rail CMOS logic and a DPA secure adiabatic logic family. From Figure 1.4 (a), we can see that the conventional CMOS based inverter has non-uniform current traces flowing in the circuit for various input transitions. Figure 1.4 (b) shows the current traces of a dual rail CMOS logic to thwart DPA attack. Though the dual rail CMOS based inverter has uniform current traces, the peak current traces is higher than the CMOS logic. Higher the peak traces, higher is the power consumption of the circuit. Further, dual rail CMOS logic family has uniform current consumption for the input transition from 0 to 1 and 1 to 0. Figure 1.4 (c) shows the DPA resistant adiabatic logic implementation of the inverter. DPA resistant adiabatic logic implementation of inverter has lower peak traces than conventional CMOS based inverter and also has uniform current traces. The uniform and lowering of peak current traces has motivated this research to explore adiabatic logic based designs to solve some of the hardware security problems in devices where power consumption is one of the most important parameters in the design.

Along with the low-power circuit design methodologies, various low-leakage emerging devices have been investigated to address the power budget issue in IoT devices. Among the various devices, FinFET devices are widely adopted by industries for the design of low power IoT nodes. FinFET has advantages such as higher on-state current, higher switching speed and low-leakage. This has motivated us to investigate the usefulness of Finfet devices in DPA secure adiabatic logic family with respect to energy-efficiency and DPA resilience property.

Recently, Magnetic Tunnel Junction (MTJ)/CMOS based Logic-in-Memory (LiM) circuits have been explored to design low-power embedded hardware. Some of the advantages of MTJ devices include non-volatility, near-zero leakage power, high integration density

and easy compatibility with CMOS devices. However, the differences in power consumption between the switching of MTJ devices increase the vulnerability of Differential Power Analysis (DPA) based side-channel attack. Further, the MTJ/CMOS hybrid logic circuits which require frequent switching of MTJs are not very energy-efficient due to the significant energy required to switch the MTJ devices. This motivated us to explore a novel method for designing cryptographic circuits utilizing the MTJ/CMOS device.

Other major hardware security concerns in IoT devices are authentication and piracy. PUFs are a class of circuits which can be used to generate a secret key for cryptographic applications to solve authentication and piracy issue. However, PUF circuit characteristics vary with the environmental variations which affects the reliability of the PUF circuit. Fuzzy extractor based Error Correction Code (ECC) have been used to correct the noisy PUF responses. Unfortunately, ECC are computationally intensive and consume high power and area which makes them not suitable to implement in IoT devices. The other main motivation of this work is to design an energy-efficient and reliable PUF which can generate reliable key for the cryptographic application in IoT devices. In this research, we have explored the time ramp voltages in adiabatic logic circuit to design energy-efficient and reliable PUF.

*In summary, this dissertation addresses the hardware security and power consumption problem in IoT devices with novel circuit design techniques in emerging transistors and non-volatile memories.*

## 1.3 Contributions

The following contributions are made in this dissertation to address the security and power consumption problems in IoT devices.

**Contribution 1:** Adiabatic logic [7] is one the circuit design techniques used to de-

sign energy-efficient hardware. In a recent seminal contribution [55] that discusses a broad range of countermeasures and their suitability for ultra-constrained devices, it is concluded that the adiabatic logic is one of the promising techniques to design energy-efficient DPA-resistant hardware. However, existing DPA resistant adiabatic logic families suffer from high non-adiabatic energy loss which reduces its energy-efficiency. In this dissertation, a novel Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) has been proposed. EE-SPFAL achieves energy-efficiency by proper switching of the transistors during the 'evaluate phase' of the clock. Further, the information leakage in EE-SPFAL is avoided by breaking the correlation between the current consumption and the input data. Basic logic cells such as buffer/inverter, AND/NAND, XOR/XNOR gates are designed using the EE-SPFAL logic. Further, the security of the proposed EE-SPFAL logic is evaluated by performing a DPA attack on the Advanced Encryption Standard (AES) S-box circuit which is designed using the EE-SPFAL gates. From our simulation based DPA attack, we have found that the EE-SPFAL based cryptographic circuits are secure against DPA attack while further lowering the power consumption compared to the CMOS based designs.

**Contribution 2:** Along with the low-power circuit design methodologies, various low-leakage emerging devices have been investigated to address the power budget issue in IoT devices. Among the various devices, FinFET devices have been widely adopted by industries for the design of low power IoT nodes. FinFET has advantages such as higher on-state current, higher switching speed and low-leakage. FinFET is a low-leakage tri-gate transistor which looks promising in the implementation of IoT devices. In this dissertation, a novel FinFET based Secure Adiabatic Logic (FinSAL) has been proposed. FinSAL has the advantage of the low-leakage properties of FinFET devices along with dynamic power savings from adiabatic logic. Further, the basic logic cells such as Buffer/NOT, XOR/XNOR and AND/NAND are designed using the FinSAL logic. Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) values are calculated to evaluate the security of

the proposed logic cells. Further, the basic logic cells such as Buffer/NOT, XOR/XNOR and AND/NAND are designed using the FinSAL logic. Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) values are calculated to evaluate the security of the proposed logic cells. Security of the FinSAL is evaluated by performing a simulation based DPA attack on a 8-bit AES S-box circuit designed using FinSAL gates. Signal-to-Noise Ratio (SNR) values of the FinSAL S-box circuit implemented at different FinFET technology nodes are also calculated.

**Contribution 3:** Recently, Magnetic Tunnel Junction (MTJ)/CMOS based Logic-in-Memory (LiM) circuits have been explored to design low-power embedded hardware. Some of the advantages of MTJ devices include non-volatility, near-zero leakage power, high integration density and compatibility with CMOS devices. However, the differences in power consumption between the change of spin orientations in MTJ devices increase the vulnerability to power analysis based side-channel attack in spin device based hardware. Further, the MTJ/CMOS hybrid logic circuits requiring frequent switching of spin orientations in MTJs are not very energy-efficient due to the significant energy required to switch the MTJ devices. We have investigated a novel approach of building cryptographic hardware in MTJ/CMOS circuits using Look-Up Table (LUT) based method where the data stored in MTJs are constant during the entire encryption/decryption operation. As a case study, we have designed a non-linear bijective function of PRESENT-80 lightweight cryptographic algorithm called substitution box or S-box and one round of PRESENT-80 cryptographic hardware using MTJ/CMOS circuits. From our simulations, it has been shown that the proposed implementation method saves significant energy compared to CMOS based designs along with this DPA resistant property.

**Contribution 4:** Currently, high supply voltage is required in both writing and sensing operations of hybrid MTJ/CMOS based LiM circuits which consumes considerable amount

of energy. In order to meet the power budget in low-power devices, it is important to investigate the novel design techniques to design ultra-low-power MTJ/CMOS circuits. We have proposed a novel Secure MTJ/CMOS Logic (SMCL) circuits. The proposed SMCL circuit saves up to 50% of energy compared to the existing state-of-art MTJ/CMOS logic by using charge sharing circuit design technique. Further, we have utilized the implementation method proposed contribution mentioned above to implement a energy-efficient and DPA secure cryptographic hardware.

**Contribution 5:** Adiabatic logic has been proposed as a novel computing platform to design energy-efficient and DPA secure IoT devices. However, IoT devices are employed in unsecured environments which leads to piracy and device authentication concerns. Physically Unclonable Functions (PUFs) have emerged as a powerful solution to a variety of security concerns such as IC piracy, IC counterfeiting, etc. PUFs have shown great promise for secure key generation for the cryptographic hardware in an inexpensive way. However, designing a reliable PUF along with energy-efficiency is a big challenge. We designed an energy-efficient and reliable PUF using adiabatic logic circuit. The proposed adiabatic PUF uses energy recovery concept to achieve high energy efficiency and uses the time ramp voltage to exhibit the reliable start-up behavior.

## 1.4 Dissertation outline

The remainder of this proposal is organized as follows: Chapter 2 describes the background and a comprehensive literature survey related to our research. In Chapter 3, we have present a novel DPA-resistant adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) family. The security of the proposed adiabatic logic family is evaluated by performing a DPA attack on the S-box circuit which is designed

using the EE-SPFAL gates. In Chapter 4, we present a novel FinFET based Secure Adiabatic Logic (FinSAL). FinSAL family has reduced dynamic and leakage power consumption as compared to existing DPA-resistant adiabatic logic family. Chapter 5 explores the novel Look-Up Table (LUT) method for implementing cryptographic hardware using non-volatile MTJ/CMOS circuits. In Chapter 6, we present a novel energy-efficient and Secure MTJ/CMOS logic. Further, energy-efficient and DPA secure lightweight PRESENT-80 cryptographic hardware has been implemented using the proposed SMCL logic. In Chapter 7, we present the design of energy-efficient and reliable Physically Unclonable Function (PUF) using adiabatic logic circuit design to address the authentication and piracy issues. Chapter 8 concludes this dissertation outlining possible future directions of this research. Content of Chapter 3 have been previously published in [37] (© 2016 IEEE).Content of Chapter 4 have been previously published in [38],[39] (© 2018 IEEE).

# Chapter 2

# Background and Related work

This chapter covers the background of adiabatic logic or energy recovery logic (low-power circuit design technique), Differential Power Analysis (DPA) attack and Physically Unclonable Function (PUF).

## 2.1 Adiabatic logic

Adiabatic logic or energy recovery logic technique is one of the low-power design techniques to design energy-efficient hardware. Adiabatic logic has reduced dynamic switching energy loss due to the recycling of charge to the power clock. Further, adiabatic logic uses time varying voltages to slowly charge and discharge the load capacitors. These time varying voltage sources can be of sinusoidal, triangular or trapezoidal voltage waveforms. The general idea behind adiabatic switching is to use a constant current source to charge the output load capacitor [72]. However, it is more practical to use a time ramp voltage source than a current source as shown in Figure 2.1.

The trapezoidal voltage ramp (Vpc) is expressed as,

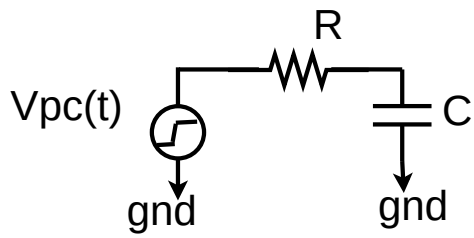



Figure 2.1: RC network charging using a trapezoidal voltage ramp.

$$\text{Vpc(t)} = \begin{cases} 0 & : \text{t} \leq 0 \\ \text{Vdd.t/T} & : 0 \leq \text{t} \leq \text{T} \\ \text{Vdd} & : \text{T} \leq \text{t} \end{cases}$$

The voltage in the load capacitor is given by,

$$V_c(t) = \begin{cases} 0 & : \text{t} \leq 0 \\ \text{C}.\frac{Vdd}{T}.(1 - e^{\frac{-t}{RC}}) & : 0 \leq \text{t} \leq \text{T} \\ \text{C}.\frac{Vdd}{T}.(1 - e^{\frac{-t}{RC}}).e^{\frac{-(t-T)}{RC}}) & : \text{T} \leq \text{t} \end{cases}$$

The energy dissipated in an adiabatic circuit when considering the charge is supplied through a constant current source is shown by,

$$E_{diss} = \frac{RC}{T} C V_{dd}^2 \tag{2.1}$$

where T is the charging/discharging time of the capacitor, C is the load capacitor, $V_{dd}$ is the full swing of the power clock. If T $\gg$ 2RC (time constant), then the energy dissipated by the adiabatic circuit is less than the conventional CMOS circuit. By choosing T $>>$ 2RC, it is possible to reduce the energy consumption compared to the conventional CMOS based logic style. Though, adiabatic circuits have reduced dynamic switching energy loss, they still suffer from other types of energy losses [31]. Further, it is also important to point out that some of the IoT devices will operate from few KHz to 10's of MHZ. For example, RFID devices will operate at 13.56 MHz. Similarly, adiabatic logic has also found many

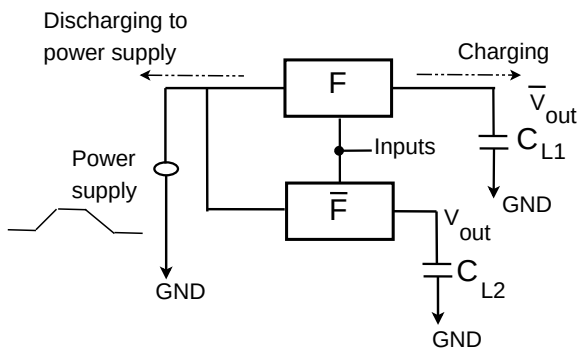



Figure 2.2: Adiabatic charging/discharging.

applications in the design of wireless medical devices such as implantable devices [65]. Adiabatic charging/discharging of the load capacitors is shown in Figure 2.2. The F shows the function to be implemented and $\overline{F}$ shows the compliment function of F.

### 2.1.1 Losses in adiabatic logic

Energy loss in adiabatic circuits can be characterized as adiabatic loss and non-adiabatic loss other than leakage loss [42].

#### Adiabatic loss

Figure 2.3(a) illustrates the switch model for the adiabatic loss. When the switch (SW) is turned ON, the adiabatic loss is given by,

$$E_{adiabatic} = \frac{R_{on}C_L}{T}CV_{dd}^2 \tag{2.2}$$

where $R_{on}$ is the ON-resistance of the switch, T is the transition period and $C_L$ is the load capacitance. From equation 2.2, it can be seen that the adiabatic loss can be eliminated, if the transition period (T) reaches infinity. In practice, it is impossible to make the transition period (T) to infinity. So, it is concluded that adiabatic loss is unavoidable.

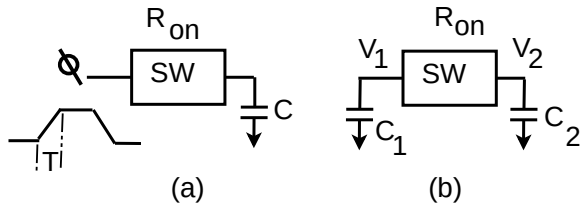



Figure 2.3: Switch model for a) adiabatic loss, b) non-adiabatic loss.

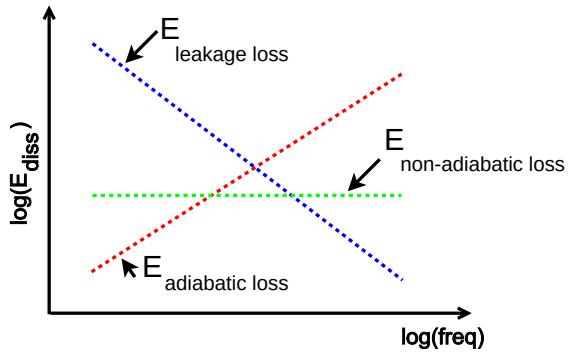



Figure 2.4: Three energy loss mechanisms in dependence of frequency [72].

**Non-adiabatic loss**

Figure 2.3(b) shows the switch model to depict the non-adiabatic loss. If any voltage difference between two terminals of a switch exists when it is turned ON, non-adiabatic loss occurs. Non-adiabatic loss is shown by

$$E_{non-adiabatic} = \frac{1}{2}\frac{C_1 C_2}{C_1 + C_2}(V_1 - V_2)^2 \tag{2.3}$$

where $C_1$ and $C_2$ are the capacitances of the two nodes connected to the switch and $V_1$ and $V_2$ are the voltages at the two nodes just before the switch is turned ON. For the low speed operation circuits, non-adiabatic loss is much higher than the adiabatic loss [42]. *In order to avoid non-adiabatic loss, the transistor should not turn ON if there is any potential difference between the drain and source (two nodes) of the transistor.*

**Leakage loss**

With the on-going shrinking of CMOS technology, leakage energy loss has become dominant over the other energy dissipation of the computing circuits. In adiabatic circuits, during each phase of the clock current flows from the voltage supply to ground, leading to the energy dissipation which cannot be recovered. All leakage mechanisms that leads to leakage current is given in mean current $\overline{I_{leak}}$. The energy consumption per cycle due to leakage loss is given by [72],

$$E_{leak} = V_{DD}\overline{I_{leak}}\frac{1}{f} \tag{2.4}$$

where $V_{DD}$ is the swing of the voltage supply, $f$ is the frequency of operation. From equation 2.4, it is inferred that leakage-related energy dissipation increases for lower frequencies. Figure 2.4 shows the three loss mechanisms with respect to frequency. Figure 2.4 shows that for lower frequencies, leakage loss and non-adiabatic loss is larger than adiabatic loss. So, reduction of leakage loss and non-adiabatic loss in adiabatic circuits for low speed circuits increases the energy efficiency.

### 2.1.2 Information leakage in low-power adiabatic logic

There are several popular adiabatic logic families that are energy-efficient in nature, however not all are suitable to design DPA-resistant hardware. For example, PFAL (Positive Feedback Adiabatic Logic) [79] and ECRL (Efficient Charge Recovery Logic) [54] are the two popular energy-efficient adiabatic logic. However, they are not suitable to build low-power DPA-resistant hardware because there is a strong correlation between the data processed and current traces during the evaluate phase. Hence, there is information leakage [9].

Figure 2.5(a) shows the schematic of the existing PFAL buffer and Figure 2.5(b) shows the timing diagram of the PFAL buffer. In the T1 phase, input is supplied to the PFAL buffer

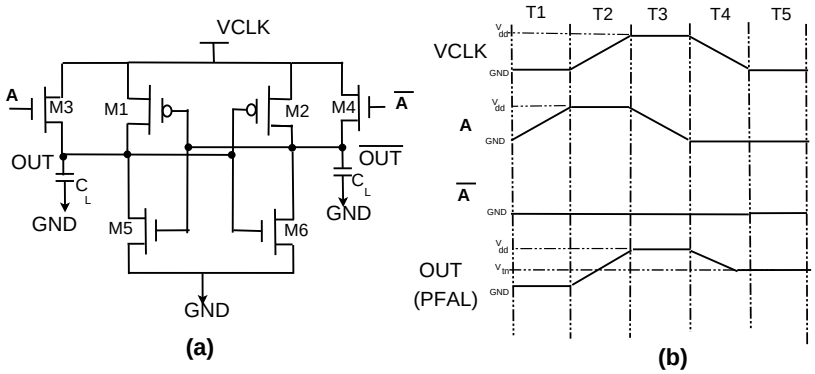



Figure 2.5: a) PFAL buffer, b) Timing digram of the PFAL buffer.

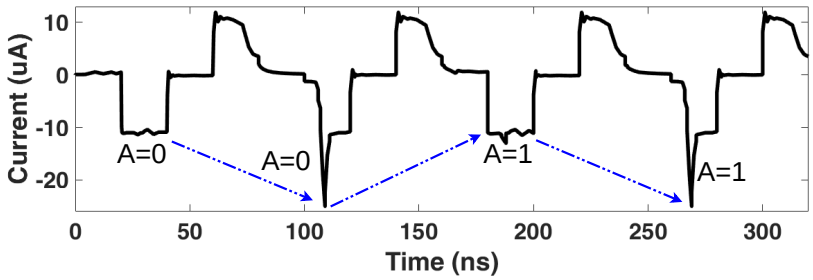



Figure 2.6: Supply current traces for the PFAL buffer.

and in the T2 phase, the inputs are evaluated and the load capacitors are charged. In the T3 phase, the outputs are held and in T4 phase, the charge is recovered. However, all the charge stored in the load capacitors are not recovered and $C.V_{tp}$ charge (C is load capacitance and $V_{tp}$ is the threshold voltage of PMOS transistor) is stored in the load capacitors at the end of the T4 phase. When the next cycle starts, and if the same inputs are passed, there will be non-uniform current consumption (Figure 2.6) due to the $V_{tp}$ charge stored at the end of the last phase. This non-uniform current consumption can be considered as a form of information leakage. We have to note that PFAL was proposed for designing low-power hardware. However, our main motivation in this work is to design low-power and secure hardware, where the information leakage through these redundant charge should be avoided. Figure 2.6 shows the information leakage in the form of non-uniform current consumption for the PFAL buffer.

## 2.2 Differential Power Analysis

Differential Power Analysis (DPA) attack is considered to be one of the most powerful side-channel attacks to reveal the secret key stored in the cryptographic device [36]. DPA attack reveals the secret key by correlating the instantaneous power consumed by the cryptographic device with the input data and the secret key. To guess the secret key, DPA uses statistical methods and evaluate the power traces with uniform plain texts. DPA requires no knowledge about the hardware implementation of the cipher and can be applied to any black box hardware implementation. These features of DPA makes it one of the powerful side channel attacks.

### 2.2.1 DPA attack flow

Advantage of DPA attack using correlation co-efficient (also known as CPA attack) is that the attacker does not need to know the internal hardware architecture to reveal the secret key. It is sufficient for the attacker to know the cryptographic algorithm which is used to encrypt/decrypt the data with the secret key. The correlation coefficient is the most common way to determine linear relationships between data. Therefore, it is an excellent choice when it comes to performing DPA attacks. Figure 2.7 shows the simulation based DPA attack flow using correlation coefficient method. DPA steps used to reveal the key are explained briefly as follows:

1. A set of plain text **I** is XORed with a set of hypothetical keys **K**. The resultant value is passed to the S-box circuit. A set of expected outputs **O** (cipher texts) from the S-box circuit (cryptographic component) is retrieved. Let $I_i$ represent an element in **I** where $i \in [0, d-1]$ and $d$ is the number of plain texts. Let $K_j$ represents an element in **K** where $j \in [0, k-1]$ where $k$ is the total number of possible keys for a S-box circuit. For an 8-bit S-box circuit, the total number of possible keys $2^8$ which is 256.

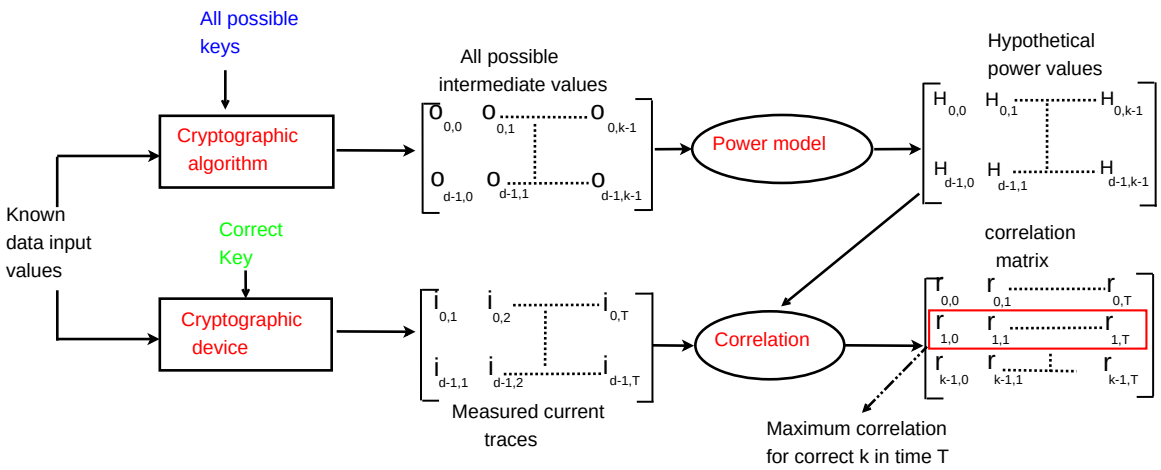



Figure 2.7: Simulation based DPA attack flow.

An element $O_{i,j}$ in the cipher texts **O** is denoted as:

$$O_{i,j} = Sbox(I_i \oplus K_j) \tag{2.5}$$

where $Sbox(.)$ represents the output of the S-box circuit.

2. The power consumption of the different runs of the plain text are recorded. The known current trace values are written as a vector **i**= $(i_1, i_2, ..., i_d)$, where $i_n$ denotes the current trace value of the $n^{th}$ input plain text. During each run of the input plain text, current traces are collected and sampled. The sampled current trace values that corresponds to a particular input plain text is given as $t_i$= $(t_{i,1}, t_{i,2}, ...., t_{i,T})$ where T denotes the length of the trace.

3. In the next step of the DPA attack, the hypothetical power consumption model is created. This model can be either Hamming Distance (HD) model or Hamming Weight (HW) model. This model is represented by the **H** matrix.

   - Hamming Distance (HD) model: The basic idea of HD model is to count the number of output transitions that occur from 0 to 1 and 1 to 0. The basic assumption of HD model is that all 0 to 1 and 1 to 0 transitions consume equal

power consumption and all 0 to 0 and 1 to 1 transitions consume equal power consumptions.

- Hamming weight (HW) model: In the HW model, the attacker assumes that the power consumption is proportional to the number of bits that are set in a processed data value. One of the limitations of HW model is, it is not well suited to describe the power consumption of the CMOS circuits. So, in this work, we have used the HD model to perform the DPA attack.

4. In the last step of the DPA attack, each column of the **H** matrix is compared with each column of the **M** matrix i.e., the hypothetical power consumption values for all the keys are compared with recorded traces at different instances of time. This will result in an another matrix **R** which is of size $K \times T$. Each element of **R** ($r_{i,j}$) contains the comparison result between the columns of $\mathbf{h}_i$ and $\mathbf{m}_j$.

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i}).(m_{d,j} - \overline{m_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})^2 . \sum_{d=1}^{D}(m_{d,j} - \overline{m_j})^2}} \tag{2.6}$$

here, $\overline{h_i}$ and $\overline{m_j}$ denote the average values of the columns $h_i$ and $m_j$ respectively.

The attacker looks for the maximal value for the entry in the matrix **R**. If the DPA attack is successful, the correct key can be identified by the maximal value that appears in a row (key) of the matrix **R**.

## 2.3 Countermeasures against DPA attack

Differential Power Analysis (DPA) attack is considered to be one of the most powerful side-channel attacks to reveal the secret key stored in the cryptographic device. Over a decade, various countermeasures have been presented in literature to counteract DPA attack. These countermeasures can be broadly classified as architecture level countermeasures, algorithmic countermeasures and the circuit level countermeasures [55].

Architecture and algorithmic countermeasures against DPA attacks are specific to a particular cryptographic algorithm and so it is difficult to automate the design flow. On the other hand, circuit level countermeasures are more generic, since they are not constrained by any algorithm.

Circuit level countermeasure against DPA attack aims to flatten the power consumption irrespective of processed data and the performed operations. Circuit level countermeasure against DPA attack can be broadly categorized into CMOS based logic style and adiabatic logic based style.

### 2.3.1 CMOS based DPA-resistant logic style countermeasure

A Sense Amplifier Based Logic (SABL) [74] was proposed by Tiri et al. in 2002 to counteract the DPA attack at the circuit level. SABL gates provide the best trade off in hardware resources, power and security, especially if balanced outputs are provided. However, the weakness of SABL is that it is sensible to unbalanced loads.

On the standard cell based implementation, Wave Dynamic Differential Logic (WDDL) [76] was proposed by Tiri et al. in 2004 where the precharge value propagates from the inputs to the outputs. Its major advantage is the use of a standard-cell flow, which facilitates the synthesis process. However, WDDL can generate glitches if it is not implemented using positive functions.

Some improvement over WDDL have been reported as Masked Dual-rail Precharge Logic (MDPL) [60] which was proposed by Popp et al. in 2005. However, the implementation of MDPL shows strong data-dependent leakage which makes them vulnerable to DPA attacks.

An enhanced SABL known as Three Phase Dual-rail Precharge Logic (TPDL) [15] was proposed by Bucci et al. in 2006. TPDL is proposed to unbalance load conditions, thus allowing a semi-custom design flow without any constraint on routing the complementary wires. The limitation of TDPL is that these designs require a third clock phase and has a

precise timing constraints. TDPL also suffers from area and energy constraint.

Random Switching Logic (RSL) [70], which was proposed by Suzuki et al. in 2007, uses a random signal to equalize the output transition probability. The main weakness of this design is that it requires strict timing.

Dual-rail Transition Logic (DTL) [56], which was introduced by Moradi et al. in 2009, aims at randomly changing the logic values and presenting the desired data at the same time. However, its effectiveness under Process Variation Temperature (PVT) is still uncertain.

Later, a delay based logic style called Delay-Based Dual-Rail Precharge Logic (DDPL) [14], was introduced by Bucci et al. in 2011, which uses random insertion of delay to mask the data. However, DDPL need level converters and requires precise timing.

**Though each secure CMOS based DPA resistant logic style has its own advantages and disadvantages, they all suffer from high power consumption which makes them not suitable for implementing in secure battery-operated IoT devices**.

Table 2.1: Drawbacks of existing DPA resistant adiabatic logic families.

| Logic family | Drawbacks |
|---|---|
| Secure Adiabatic Logic (Khatir et al., 2008) [34] | High area and exhibit current to input data dependency |
| Symmetric Adiabatic Logic (Choi et al., 2010) [19] | Outputs are not stabilized during charge sharing phase |
| Charge Sharing Symmetric Adiabatic Logic (Monteri et al., 2013) [51] | High area and more complicated to design |
| Secure Quasi Adiabatic Logic (Avital et al., 2015) [9] | Suffers from non-adiabatic energy losses |
| Bridge Boost Logic (Lu et al., 2015) [43] | Relatively high energy consumption |

### 2.3.2 Adiabatic logic based DPA-resistant logic style countermeasure

Adiabatic logic is a low power technique which can be used to design low power hardware. Very few contributions have been made in the area of designing low power and secure hardware.

Khatir et al. has proposed a secure adiabatic logic (SAL) [34] in 2008, which uses the

charge recovery logic style to design energy-efficient and DPA secure hardware. However, SAL uses 8 phase clocks which increases the area. Further, SAL also exhibited current-data dependency which makes SAL hardware vulnerable to DPA attack.

Later, Symmetric Adiabatic Logic (SyAL) [19] was introduced by choi et al., which modifies the popular charge recovery logic, called Efficient Charge Recovery Logic (ECRL), to make it secure. This logic uses symmetric discharge paths and charge sharing feature to equalize the voltage between the output nodes and the internal nodes. This feature balances the supply current waveforms of this logic. However, a drawback is that the outputs of SyAL are not stabilized during the charge-sharing phase.

In order to overcome the drawback of SyAL, Monterio et al. proposed Charge Sharing Secure Adiabatic Logic (CSSAL) [51] in 2013. This logic is implemented with charge sharing symmetric input logic structure in SyAL. But CSSAL uses twelve trapezoidal clock sources making their structure more complicated.

Avital et al. has proposed Secure Quasi Adiabatic Logic (SQAL) [9], which modifies the ECRL logic to make it secure with an additional discharge phase. Though SQAL has reduced area and improved security over all the presented DPA resistant adiabatic logic families, it suffers from other adiabatic energy losses such as non-adiabatic energy loss. Table 2.1 shows the disadvantages of the existing adiabatic logic based DPA-resistant logic style.

Lu et al. has proposed Bridge Boost Logic (BBL) [43] which is supposed to provide DPA resistant solution for high speed circuits. However, BBL has relatively high power consumption compared to existing DPA-resistant adiabatic logic. High power consumption makes it not suitable to implement in IoT devices.

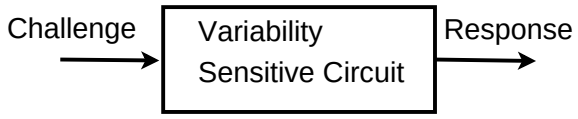



Figure 2.8: PUF production using inherent variations.

## 2.4 Physically Unclonable Function

Apart from energy-efficiency, IoT devices also suffer from piracy and authentication problems as these devices are employed in unsecured environments. In recent years, PUFs have emerged as a powerful solution to a variety of security concerns such as IC piracy, IC counterfeiting, etc[69]. PUFs are a class of circuits that use the inherent variations in an Integrated Circuit (IC) manufacturing process to create unique and unclonable IDs. PUFs also play a major role in secure authentication and key management in cyber-physical security and IoT devices. PUF can also be considered as a promising solution for authentication in IoT devices [58]. A PUF is provided with challenge bits (C) and due to the intrinsic variations in the IC manufacturing process, it results in unpredictable outputs called response bits (R). The uncontrollable IC manufacturing errors make the PUF response to be unique and unclonable. Figure 2.8 shows the block diagram for PUF production using inherent variations. Hence, a PUF can be considered as a fingerprint for CMOS ICs. Moreover, PUF outputs are hard to predict, simulate or emulate.

PUFs are generally classified into two types namely weak and strong PUFs depending on the number of challenges that can given to the PUF and the number of responses it can generate [18]. Strong PUFs have exponential challenge and response pairs which make them to be used for challenge response pair based authentication. Some of the example of strong PUF include arbiter PUF, Ring Oscillator PUF etc. Weak PUFs have limited challenge response pairs which make them useful for key generation in cryptographic applications [27] [29]. An example of weak PUF is SRAM PUF [78]. As an example, operation of SRAM PUF is described below.

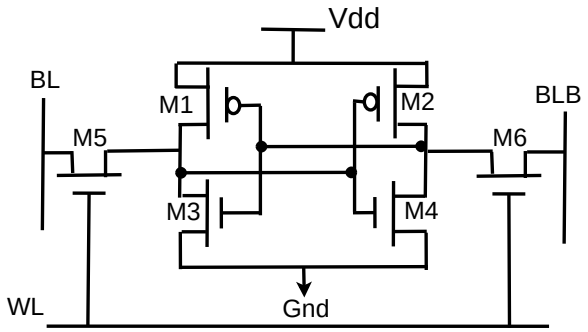



Figure 2.9: SRAM PUF cell.

### 2.4.1 SRAM PUF

This section describes the background on SRAM PUF [29]. Figure 2.9 shows the schematic of the 6T SRAM PUF cell. The 6T SRAM cell consists of a bistable circuit which has two cross coupled inverters (M1, M2, M3 and M4). When the SRAM cell is powered, current will start flowing through M1 and M2. Due to intrinsic variations in the transistors, the threshold voltage of one PMOS will be higher than the other. So, more current will start flowing through the PMOS with lower resistance and hence one output will be biased towards logic "1" while the other output will be at logic "0". Since both the inverters are designed to be identical in strength, the output response will be determined by the intrinsic process variations.

Though SRAM PUF has several advantages such as low-power, high density, etc., the reliability is one of the major concern in the design of PUF in particular for key generation application. Cortez et al. [21] has reported that intelligent choosing of time ramp up at a particular temperature can improve the reliability of SRAM PUF cells. However, this technique requires additional circuitry to perform the intelligent time ramp up operation to improve the reliability of SRAM PUF cell. Similarly, Vijayakumar et al. [80] have proposed a majority voting technique to improve the reliability of the SRAM PUF. However, this technique requires multiple turning on and turning off of the SRAM cell.

### 2.4.2 Metrics for evaluating the PUF

This section discusses the metrics used to evaluate the performance of PUF.

#### Uniqueness

Uniqueness is used to determine the ability of a PUF to uniquely distinguish a chip among the group of other chips. The ideal value of the uniqueness metric is 50 %. If two different PUF instances (i and j), have responses $R_i$ and $R_j$ which is of bit length "n", then uniqueness is given by,

$$Uniqueness = \frac{2}{k(k-1)} \Sigma_{i=1}^{k-1} \Sigma_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\% \tag{2.7}$$

where HD($R_i, R_j$) represents the Hamming Distance (HD) between $R_i$ and $R_j$. k represents the total number of IC chips.

#### Uniformity

Uniformity is used to measure whether the number of zeros and number of ones in the response bits are balanced or not. Uniformity is given by measuring number of 1's in the proposed 128-bit PUF. Uniformity is given by,

$$Uniformity = \frac{1}{n \times k} \Sigma_{i=1}^{k-1} r_{i,l} \times 100\%, \tag{2.8}$$

where $r_{i,l}$ represents the l-th bit from PUF instance i.

#### Reliability

The reproducibility of the response bits from the same PUF instance with the varying environmental conditions such as temperature, supply voltage is given by reliability metrics. For $i^{th}$ PUF instance, let $R_i$ be the reference response or the golden response recorded under nominal operating conditions. Then, applying the same challenge to the same PUF but

under different environmental conditions, n responses are observed. Reliability metric is given by,

$$Reliability = [1 - \frac{1}{k}\Sigma_{i=1}^{k}\frac{HD(R_i, R_{i,t}^{'})}{n}] \times 100\% \tag{2.9}$$

where HD($HD(R_i, R_{i,t}^{'})$ is the HD between the golden response and the response generated by the same PUF instance at different environmental conditions. In other words, reliability is the measure of total number of bits flipped between the golden response and the response recorded from the same PUF instance with different environmental conditions. The ideal value of the reliability metric is 100 %.

# Chapter 3

# Energy-Efficient Secure Positive Feedback Adiabatic Logic

The emergence of Internet of Things (IoT) have increased the need of Radio Frequency Identification (RFID) and smart cards that are energy-efficient and secure against Differential Power Analysis (DPA) attacks. Adiabatic logic is one of the circuit design techniques that can be used to design energy-efficient and secure hardware. However, the existing DPA resistant adiabatic logic families suffer from non-adiabatic energy loss. This chapter presents a novel adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) family that is energy-efficient compared to the state-of-art designs and also is secure against DPA attacks. Energy-efficiency of the EE-SPFAL is improved by reducing the non-adiabatic energy loss. Further, EE-SPFAL is secure against DPA as it breaks the correlation between the power consumption and the data being processed.

## 3.1 Logic structure of EE-SPFAL gates

Figure 3.1(a) shows the schematic diagram of the proposed EE-SPFAL buffer. The proposed buffer is modified from the Positive Feedback Adiabatic Logic (PFAL) [79]. In

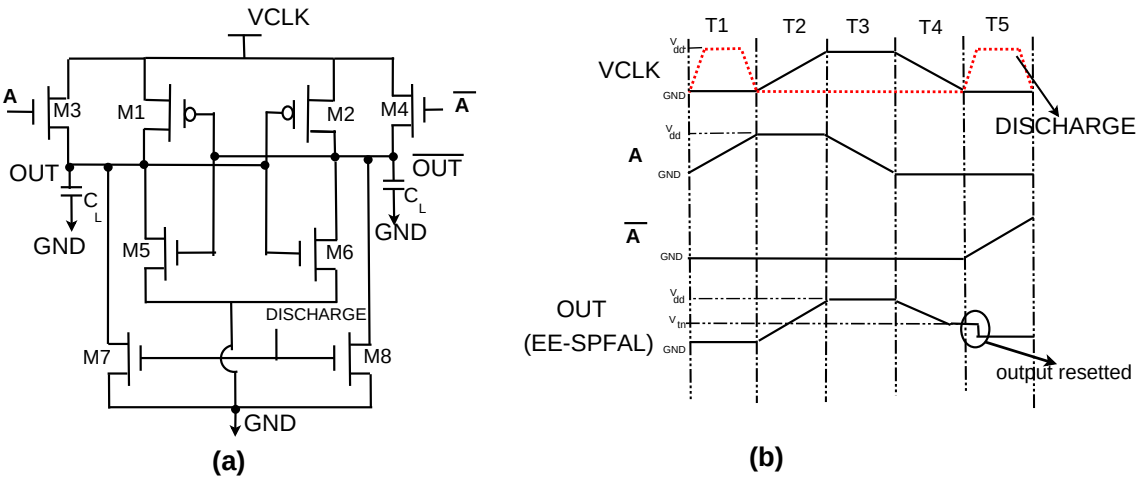



Figure 3.1: a) Proposed EE-SPFAL buffer, b) Timing digram of the EE-SPFAL buffer.

Figure 3.1(a), M1 and M2 are used to recover the charge from the load capacitors. M3 and M4 are the evaluate transistors which are used to perform the logical operation. M7 and M8 are used to reset the outputs. M5 and M6 are used to avoid the minimal logical degradation. In this research, we are solving the leakage of information in PFAL by equalizing the load voltage before evaluating the next cycle. In this case, we are resetting the output before the evaluation of the next cycle. Timing diagram of the proposed EE-SPFAL buffer is shown in Figure 3.1(b).

Let us try to understand the operation of the EE-SPFAL buffer through different phases (wait, evaluate, hold, recovery) of the clock. Let us assume that all the nodes are at GND (zero potential) initially.

**T1 (Wait phase ):** At T1, VCLK is at GND (Figure 3.1 (b)). Input A slowly rises from GND to $V_{dd}$. As we have assumed that all the node potentials are at GND initially, M3 is turned ON without non-adiabatic loss. M7 and M8 are turned ON to discharge the redundant charge stored in the previous phase of the operation. The rest of the transistors are turned OFF in this phase. Figure 3.2 shows the switching operation of the transistor in the T1 phase.

**T2 (Evaluate phase):** At T2, the DISCHARGE signal is at GND. A is at $V_{dd}$ and VCLK rises from GND to $V_{dd}$. VCLK acts as the source node and OUT acts as the drain

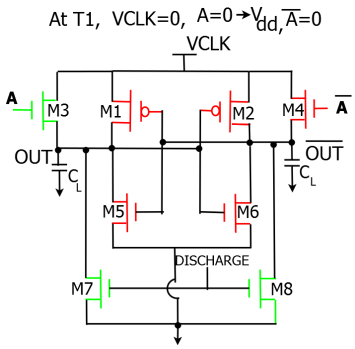



Figure 3.2: Switching operation of transistors in the T1 phase of EE-SPFAL buffer for A=1, Ā=0.

node for the M1 transistor. When VCLK rises from GND to $V_{tp}$, current will flow through M3 to charge the load capacitor without non-adiabatic loss (Figure 3.3a). PMOS will be turned ON if $V_{SG_p}$ is greater than $V_{tp}$. For M1 to be turned ON, $V_{SG_p} > V_{tp}$.

$$V_{S_{M1}} - V_{G_{M1}} > V_{tp}$$

For M1, $V_{S_{M1}} = V_{VCLK}$, $V_{G_{M1}} = V_{\overline{out}}$.

$$V_{VCLK} - V_{\overline{out}} > V_{tp}$$

Since, $V_{\overline{out}} = 0$, the above equation can be written as,

$$V_{VCLK} > V_{tp} \tag{3.1}$$

When the clock reaches $V_{tp}$, M1 will be turned ON. The current will flow through both M1 and M3 to charge the load capacitor without non-adiabatic loss (Figure 3.3b). When OUT reaches $V_{tn}$, M6 is turned ON and the redundant voltage at $\overline{out}$ is discharged to GND. M3 will be turned OFF if $V_{GS_n} < V_{tn}$.

$$V_{G_{M3}} - V_{S_{M3}} < V_{tn}$$

For M3, $V_{G_{M3}} = V_{dd}$ and $V_{S_{M3}} = V_{out}$

$$V_{dd} - V_{out} < V_{tn}$$

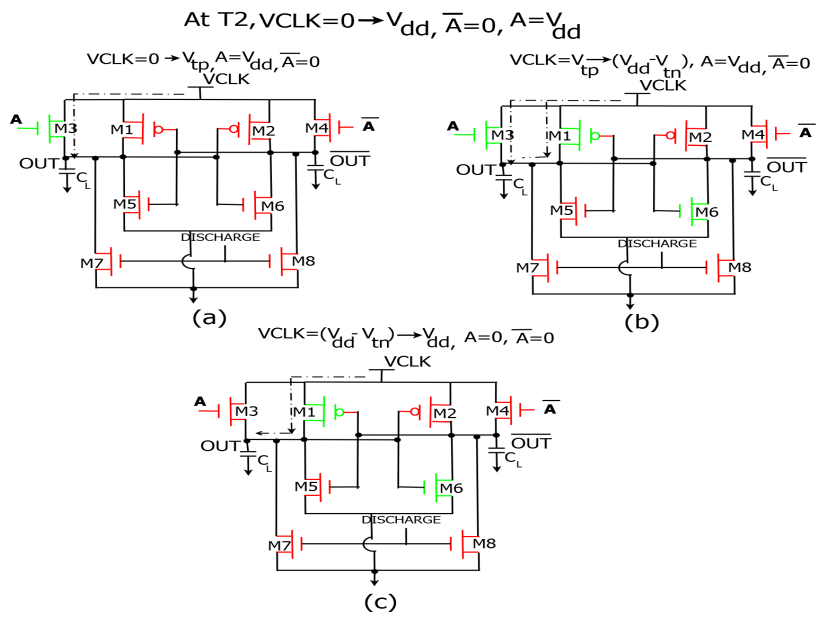



Figure 3.3: Switching operation of transistors in the T2 phase of EE-SPFAL buffer for A=1, Ā=0. (a) represents the switching operation of the transistors when VCLK reaches $V_{tp}$ from GND. (b) represents the switching operations when VCLK reaches from $V_{tp}$ to $V_{dd} - V_{tn}$. (c) represents the switching operations when VCLK reaches $V_{dd}$ from $V_{dd} - V_{tn}$.

Rearranging the above equation, we get

$$V_{out} > V_{dd} - V_{tn} \tag{3.2}$$

When OUT reaches $V_{dd} - V_{tn}$, M3 will be turned OFF and the current will flow through M1 to charge the load capacitor (Figure 3.3c).

**T3 (Hold Phase):** At T3, the clock VCLK is at $V_{dd}$. Input A is slowly decreased from $V_{dd}$ to GND. The output will be hold.

**T4 (Recovery Phase):** At T4, the clock VCLK slowly decreases from $V_{dd}$ to GND. The charge stored in the output load capacitor is slowly recovered back to the clock through M1. The recovery of charge continues until the M1 transistor is turned OFF. In this phase, the clock will follow the OUT node, as the potential of the OUT node is greater than the potential of the clock. So, the OUT node acts as the source for the transistor M1 and the

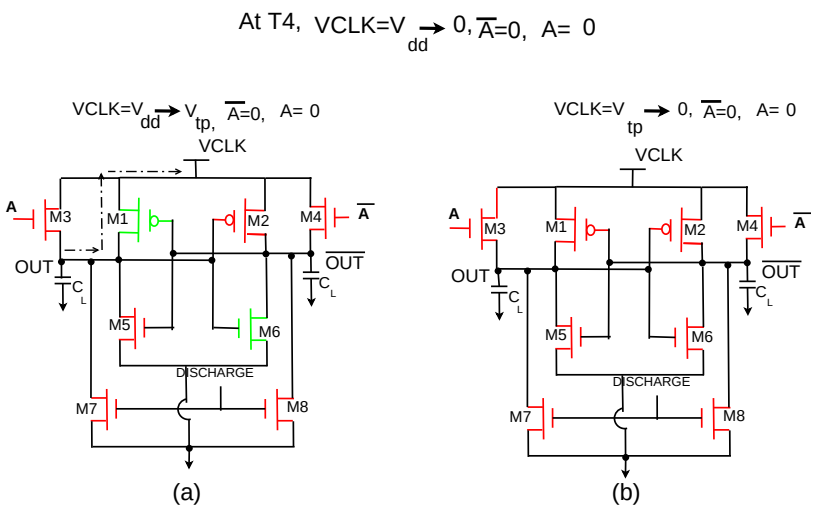



Figure 3.4: Switching operation of transistors in the T4 phase of EE-SPFAL buffer for A=1, Ā=0, (a) represents the switching operation of the transistors when VCLK reach $V_{tp}$ from $V_{dd}$, (b) represents the switching operation of the transistors when VCLK reach GND from $V_{tp}$.

clock VCLK acts as the drain for M1. Figure 3.4 shows the switching operation of the transistors in T4 phase. PMOS will be turned OFF when $V_{SG_p}$ is less than $V_{tp}$.

$$V_{SG_p} < V_{tp}$$

$$V_{S_{M1}} - V_{G_{M1}} < V_{tp}$$

In this phase, $V_{S_{M1}} = V_{out}$ and $V_{G_{M1}} = 0$ for M1.

$$V_{out} - 0 < V_{tp}$$

$$V_{out} < V_{tp} \tag{3.3}$$

When the output voltage reaches $V_{tp}$, M1 is turned OFF and the output voltage will stay at $V_{tp}$ at the end of this phase.

Charges stored in the output node at the end of the 1st cycle (T1-T4) is discharged to the ground in the next phase of the clock (T5) through M7 or M8 by using the discharge signal (Figure 3.1(b)). Resetting the output node to zero reduces the correlation between the current supplied and the data evaluated.

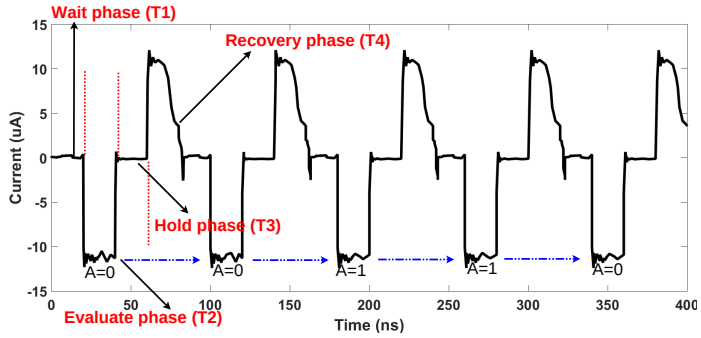



Figure 3.5: Supply current traces for the EE-SPFAL buffer.

Figure 3.5 shows the supply current traces for the EE-SPFAL buffer with the load capacitance of 100fF. It is shown that for the various input transitions, EE-SPFAL buffer consumes uniform current. Current consumption in each phase (wait, evaluate, hold, recovery) of the clock is also shown in the Figure 3.5.

### 3.1.1 Energy Analysis of buffers

In this work, energy consumption of EE-SPFAL buffer is compared with a DPA resistant adiabatic logic called Secure Quasi-Adiabatic Logic (SQAL) family. SQAL [9] has less area and energy consumption compared to Symmetric Adiabatic Logic (SyAL) [19] and Charge Sharing Secure Adiabatic Logic (CSSAL) [51]. However, SQAL, CSSAL, and SyAL logic styles suffer from non-adiabatic loss during the evaluate phase of the clock. It should be noted that the timing diagram of the SQAL buffer is similar to that of EE-SPFAL buffer as shown in Figure 3.1(b). During the evaluate phase of the clock, the load capacitors in the SQAL buffer are abruptly charged to $V_{tp}$ leading to $2X(\frac{1}{2})CV_{tp}^2$ Joules of non-adiabatic energy loss per bit operation. In the EE-SPFAL buffer, the non-adiabatic energy loss is avoided during the evaluate phase by not turning ON the transistor when there is any potential difference between the two nodes (drain and source) of the transistor. For example, in the EE-SPFAL buffer, transistor M3 or M4 is turned ON when there is no potential difference between its source and drain. So, the load capacitors are charged without any non-adiabatic energy loss.

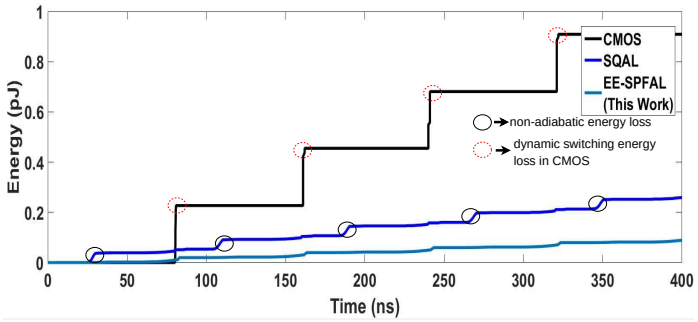



Figure 3.6: Energy consumed in each cycle of CMOS, SQAL and EE-SPFAL buffer.

Figure 3.6 shows the energy consumed during each cycle of the CMOS, SQAL, and EE-SPFAL buffers. The simulations are performed at 12.5 MHz, the period of each cycle is 80ns. Each phase (hold, evaluate, wait and recover) of the clock is 20ns each. It can be seen that during the evaluate phase of the clock (20ns-40ns for the first cycle), the SQAL buffer consumes more energy than the EE-SPFAL buffer.

### 3.1.2 Logic gates using EE-SPFAL

Figure 3.7(a) shows the schematic diagram of the XOR/XNOR gate and Figure 3.7(b) shows the schematic diagram of the AND/NAND gate. Figure 3.8(a) shows the layout of the XOR/XNOR gate and Figure 3.8(b) shows the layout of the AND/NAND gate. The logic function of the EE-SPFAL gates are symmetrically built to balance the load capacitances. For instance in Figure 3.7(a), we can see that the pull up network of the XOR logic function consists of two series transistors (M3 and M4) and a parallel transistor (M5). Similarly, the pull up network of the XNOR logic function in Figure 3.7(a) consists of two series transistor (M6 and M7) and a parallel transistor (M8). Thus, the load capacitance of the EE-SPFAL based XOR/XNOR gate is balanced. The logic function of the AND/NAND gate as shown in Figure 3.7(b) can be designed using M3, M4, M8 and M10. The pull up network of the AND logic function can be designed by connecting the M3 and M4 transistors in series. Similarly, the pull up network of the NAND logic function can be designed by connecting the M8 and M10 transistors in parallel. However, the overall load capaci-

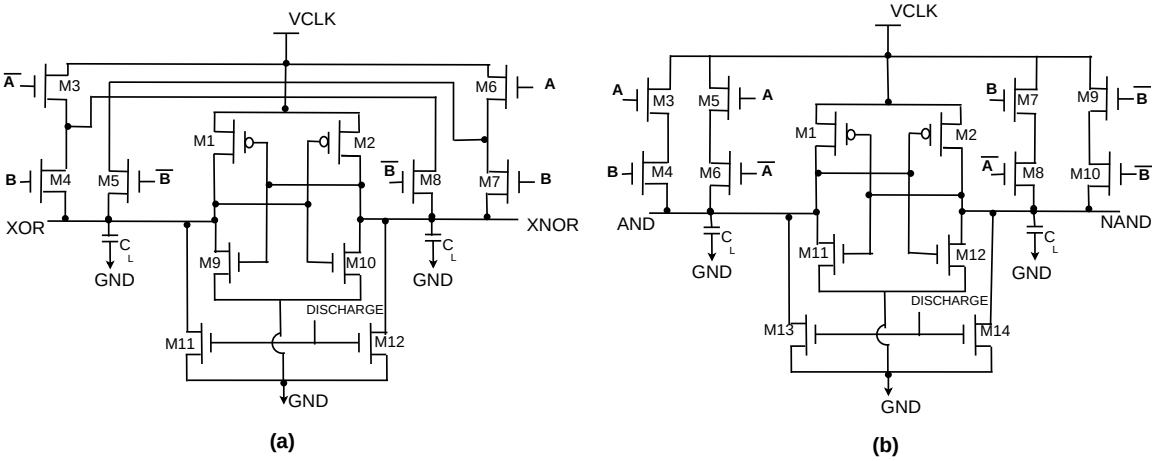



Figure 3.7: Schematic diagram of EE-SPFAL based a) XOR/XNOR gate, b) AND/NAND gate.

tance of the AND logic function is not same as the overall load capacitance of the NAND logic function. In order to balance the load capacitance, M5, M6, M7 and M9 transistors are added. These transistors are connected in such a way that the overall load capacitances of the AND and NAND logic functions are balanced while the functionality of the circuit remains the same.

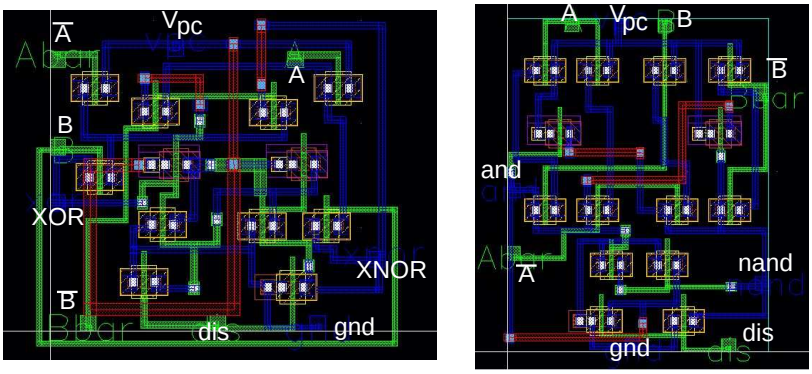
Table 3.1 shows the transistor count comparison of different DPA resistant families. EE-SPFAL, SQAL, CSSAL, and SyAL are DPA-resistant adiabatic logic families. The transistor counts are also compared with the CMOS based DPA resistant logic family called Sense Amplifier Based Logic (SABL) [76]. It is clear from the table, that EE-SPFAL logic requires fewer transistors compared to other DPA-resistant adiabatic logic families except for SQAL. However, EE-SPFAL consumes less energy as compared to SQAL due to the reduction of non-adiabatic energy loss. It has to be noted that EE-SPFAL requires less transistors as compared to the SABL logic family. Though DPA-countermeasure circuits have area overhead, they provide resistance against DPA-attacks. In order to reduce the area overhead of these logic families, emerging nano-transistors based designs need to be investigated.

Table 3.1: Transistor count comparison for DPA resistant families

| **Logic family** | **Logic gate** | **Transistor count per gate** |
|---|---|---|
| **EE-SPFAL** | BUFFER | 8 |
| | XOR | 12 |
| | NAND | 14 |
| **SQAL[9]** | BUFFER | 5 |
| | XOR | 9 |
| | NAND | 13 |
| **CSSAL[51]** | BUFFER | 11 |
| | XOR | 21 |
| | NAND | 21 |
| **SyAL[19]** | BUFFER | 5 |
| | XOR | 15 |
| | NAND | 15 |
| **SABL[76]** | BUFFER | 14 |
| | XOR | 18 |
| | NAND | 18 |

## 3.2 Simulation results of EE-SPFAL based logic gates

In this section, we present the simulation results of the EE-SPFAL logic gates and other existing DPA-resistant adiabatic logic families. Simulations are done in Cadence Virtuoso using $180nm$ technology with the load capacitance of 100fF. The parameter Normalized Energy Deviation (NED), defined as $(E_{max} - E_{min})/E_{max}$, is used to indicate the percentage difference between minimum and maximum energy consumption for all possible input transitions. Normalized Standard Deviation (NSD) indicates the energy consumption variation based on the inputs and it is calculated as $\frac{\sigma_E}{\bar{E}}$. $\bar{\text{E}}$ denotes the average energy dissipation for various input transitions. In general, '$n$' input gate will have $2^{2n}$ possible input transitions. For example, 2 input gates will have 16 input transitions. $\sigma_E$ denotes the standard deviation of the energy consumed by the circuit and it is given by $\sqrt{\frac{\sum_{i=1}^{n}(E_i-\bar{E})^2}{n}}$. The calculated values of NED and NSD for the proposed XOR gate and AND gate show the ability of the proposed logic family to resist DPA attacks.




(a) (b)

Figure 3.8: Layout of a) XOR/XNOR gate, b) AND/NAND gate.

Table 3.2: Simulated and calculated results for XOR gate for various DPA-resistant adiabatic logic families.

| Logic family | SyAL [19] | CSSAL [51] | SQAL [9] | EE-SPFAL |
|---|---|---|---|---|
| $E_{min}$(pJ) | 0.68 | 2.3 | 1.38 | 0.19 |
| $E_{max}$(pJ) | 1.98 | 2.8 | 1.4 | 0.2 |
| NED (%) | 49 | 0.92 | 0.07 | 0.01 |
| NSD(%) | 25.39 | 0.32 | 0.01 | 0.05 |

Table 3.2 and Table 3.3 show the simulated and calculated values for the various DPA-resistant adiabatic logic based XOR and AND gates respectively at 12.5 MHz. It can be seen from Table 3.2 and Table 3.3 that for various transitions of the input bits, our EE-SPFAL based XOR and AND gate consume uniform energy. NED and NSD values of EE-SPFAL based logic gates are less than 1%. The minimum value of NED and NSD values show that the EE-SPFAL based logic gates balance the energy consumption for various input transitions. It can also be seen that the maximum energy consumption of the proposed EE-SPFAL based logic gates are lower than that of the other DPA-resistant adiabatic logic families.

Table 3.3: Simulated and calculated results for AND gate for various DPA-resistant adiabatic logic families.

| Logic family | SyAL [19] | CSSAL [51] | SQAL [9] | EE-SPFAL |
|---|---|---|---|---|
| $E_{min}$(pJ) | 0.7 | 2.14 | 1.9 | 0.24 |
| $E_{max}$(pJ) | 1.96 | 2.17 | 2.3 | 0.29 |
| NED (%) | 50.8 | 1.2 | 1.8 | 0.18 |
| NSD(%) | 23.32 | 0.04 | 0.09 | 0.05 |

## 3.3 Leakage current analysis of EE-SPFAL logic gates

In this section, leakage current consumption of the EE-SPFAL logic gates is presented along with some of the state-of-art DPA-resistant adiabatic logic families.

Table 3.4: Leakage current of various DPA resistant adiabatic logic families (AND gate).

| Logic family | SyAL [19] | CSSAL [51] | SQAL [9] | EE-SPFAL |
|---|---|---|---|---|
| Leakage current (A=0, B=0) | 68.7 nA | 64.93 nA | 68.1 nA | 73.6 nA |
| Leakage current (A=0, B=1) | 70.5 nA | 66.2 nA | 70.91 nA | 76.9 nA |
| Leakage current (A=1, B=0) | 75 nA | 70.3 nA | 72.8 nA | 76.03 nA |
| Leakage current (A=1, B=1) | 69.2 nA | 65.42 nA | 73.4 nA | 76.4 nA |
| Average Leakage current | 70.85 nA | 66.71 nA | 71.3 nA | 75.73 nA |

In measuring the leakage current of the DPA-resistant adiabatic logic families, a constant input is applied to the logic gates. Leakage current for the adiabatic logic gates are the mean of the leakage current flowing during the evaluate, hold, and recovery phases of the clock [72]. To the best of our knowledge, there is not much work done on leakage current consumption analysis of the DPA resistant adiabatic logic gates.

Table 3.4 and Table 3.5 shows the leakage current consumption of the various DPA resistant adiabatic logic based AND and XOR gates respectively. From our simulation results, it has been inferred that the EE-SPFAL logic gates consume more leakage current compared to SyAL, CSSAL and SQAL based logic gates. SyAL, CSSAL, and SQAL logic

families are designed based on Efficient Charge Recovery Logic (ECRL)[54] family. ECRL logic family is a differential cascode voltage switch logic based low-power circuits which makes ECRL family to consume less leakage current as compared to PFAL logic. EE-SPFAL logic is based on PFAL based logic family. EE-SPFAL has more leakage current flowing through the circuit due to the additional ground paths associated with each gates. We have to remember that transistors M9 and M10 in Figure 3.7(a) and M11 and M12 in Figure 3.7(b) are used to avoid the logical degradation of the signal. Transistors M11 and M12 in Figure 3.7(a) and M3 and M14 in Figure 3.7(b) are used to reset the outputs to make the gates more secure against DPA attacks. However, these transistors are increasing the leakage current flow in the proposed EE-SPFAL based logic gates.

Table 3.5: Leakage current of various DPA resistant adiabatic logic families (XOR gate).

| Logic family | SyAL [19] | CSSAL [51] | SQAL [9] | EE-SPFAL |
|---|---|---|---|---|
| Leakage current (A=0, B=0) | 72 nA | 66 nA | 129.2 nA | 136.01 nA |
| Leakage current (A=0, B=1) | 71.3 nA | 65.5 nA | 124.82 nA | 136.05 nA |
| Leakage current (A=1, B=0) | 71.2 nA | 65.43 nA | 115.6 nA | 136.02 nA |
| Leakage current (A=1, B=1) | 72.5 nA | 66.2 nA | 132.3 nA | 136.09 nA |
| Average Leakage current | 71.75 nA | 65.78 nA | 125.5 nA | 136.04 nA |

## 3.4 Energy-efficiency and security evaluation of EE-SPFAL logic family

In this section, we discuss the security evaluation of the proposed EE-SPFAL logic. We have implemented a Positive Polarity Reed Muller (PPRM) architecture based S-box circuit [57] (Figure 3.10) using EE-SPFAL gates and performed DPA attack on it. It is shown that the EE-SPFAL based S-box circuit is more energy-efficient compared to the existing

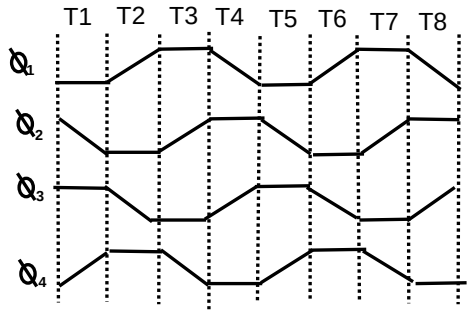



Figure 3.9: 4-phase clocks used to build complex circuit using EE-SPFAL logic.

DPA-resistant adiabatic logic and non-adiabatic logic families and is resistant against DPA attack. We have also implemented first round of AES algorithm using EE-SPFAL gates.

### 3.4.1 Implementation of PPRM based S-box circuit using EE-SPFAL logic

In a cryptographic algorithm such as Advanced Encryption Standard (AES) [61], the S-box is the key component for the encryption/decryption operations. S-box is a single non-linear hardware block which performs non-linear operation in the AES algorithm. In the AES algorithm, the input byte (8-bits) is replaced by the output of the S-box circuit. However, the S-box is prone to DPA attacks due to its huge power consumption. For example, 75% of the total power consumption in implementing the AES algorithm is consumed by the S-box circuit [57]. In order to reduce the power consumption of the S-box circuit and to improve its resistance against DPA attacks, we implemented the PPRM based S-box circuit using EE-SPFAL logic.

As we discussed earlier, EE-SPFAL logic uses 4 phase trapezoidal clocks to recover the energy. To implement a PPRM based S-box circuit using EE-SPFAL gates, four trapezoidal power clocks (as shown in Figure 3.9) which are 90 degrees in advance of each other is employed. Each stage of the S-box circuit is connected to the power clock which has one phase latency with respect to its previous stage. The output of EE-SPFAL logic is valid after one phase cycle of the clock. So, in the implementation of the S-box circuit using

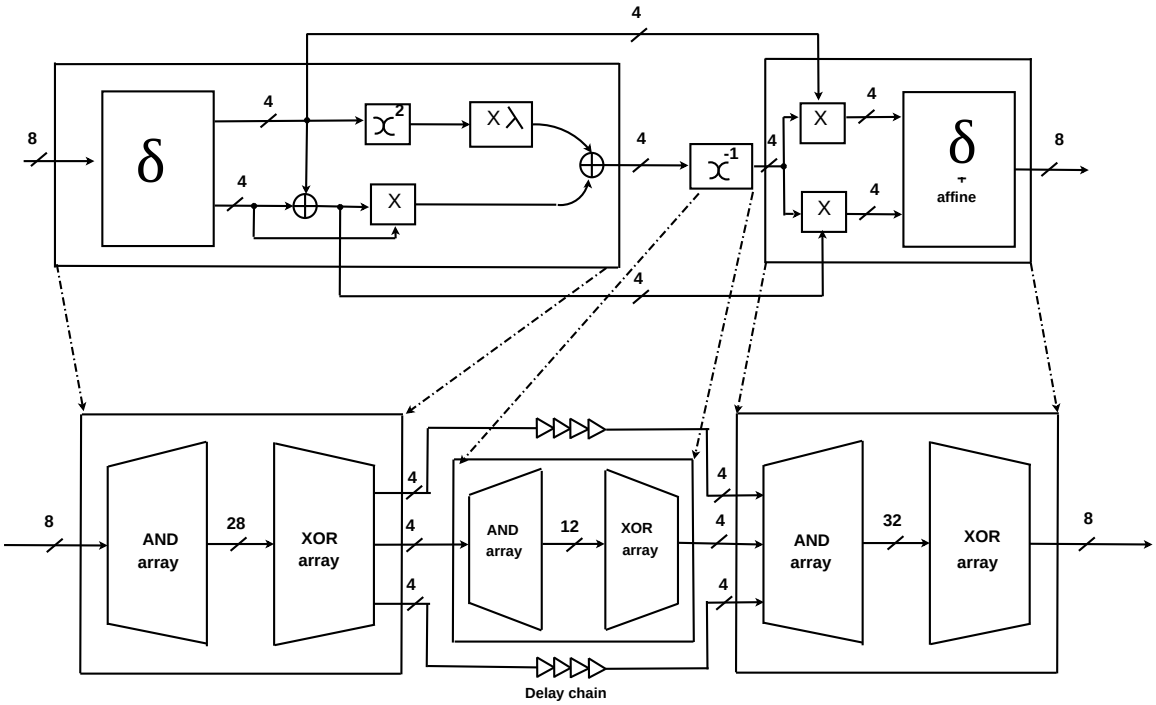



Figure 3.10: A Positive Polarity Reed Muller (PPRM) architecture based S-box circuit. [57]

EE-SPFAL logic, additional buffers are inserted to synchronize the clocks. We used 135 EE-SPFAL XOR gates and 97 EE-SPFAL NAND gates to implement the PPRM based S-box circuit. 185 additional buffers have been used to synchronize the clocks in the EE-SPFAL implementation of the PPRM based S-box circuit.

From our simulation results, we found that the PPRM S-box circuit implemented using EE-SPFAL logic consumes 19.8$\mu$W on average at 12.5 MHz and the CMOS implementation of PPRM S-box circuit consumes 54$\mu$W on average at 12.5 MHz. It is shown that the EE-SPFAL based S-box circuit saves 64% of average power compared to its CMOS implementation at 12.5 MHz.

### 3.4.2 Test case for EE-SPFAL based S-box circuit

DPA attack for the EE-SPFAL based S-box circuit and conventional CMOS based S-box circuit have been performed as described in chapter 2. In our first test case, the key was

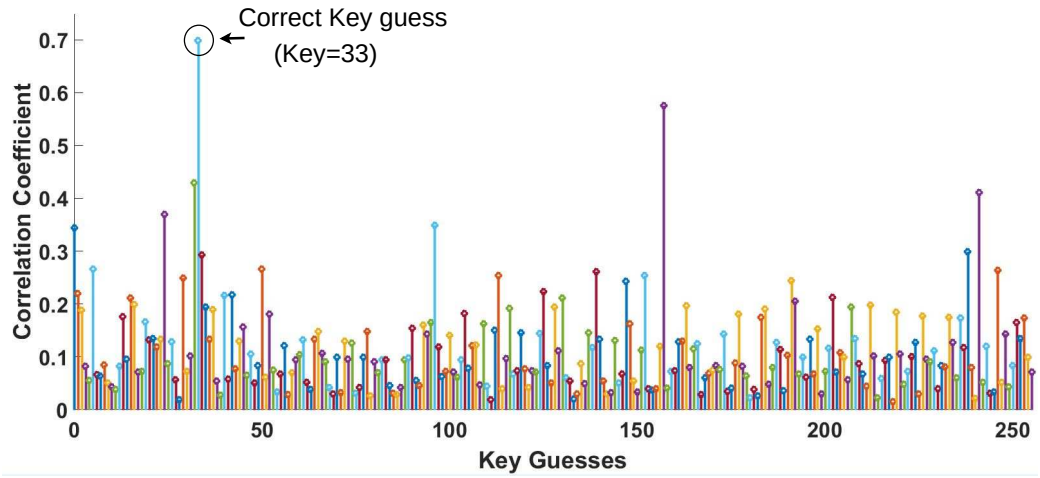



Figure 3.11: A successful DPA attack on S-box circuit implemented using CMOS implementation with key=33.

chosen to be $(33)_{10}$. A DPA attack was performed on EE-SPFAL, SQAL, and CMOS based test circuits. Test circuit consisted of eight XOR gates performing Add Round Key operation and the PPRM based S-box circuit together. In the real world DPA attacks, a large number (greater than 100,000 plain texts) of plain texts are fed as input to the crypto processor. However, in this research, we are performing the simulation based DPA attack without any electrical noises. Moreover, test chip was not a full chip with other analog and digital modules of the crypto processor that consume additional current. So, for our CMOS based S-box circuit, the secret key was revealed using fewer number of traces (512 input traces). We have to note, that the electrical noises present in the chip increases the number of traces required to break the crypto processor [50]. For our test case simulations, we consider the ideal environment (without noise) for an attacker to perform DPA attack. The same environment has been used to design SQAL and EE-SPFAL based S-box circuit. As seen from Figure 3.12 DPA attack was unsuccessful on EE-SPFAL based S-box circuit. Further, we have also tested our designs by providing up to 20,000 input traces and we found that the key was not revealed in the test circuit built using EE-SPFAL logic gates.

Figure 3.11 shows the correlation coefficient values of the hypothetical key guesses for successful DPA attack using CMOS logic. It can be seen that the correlation co-efficient

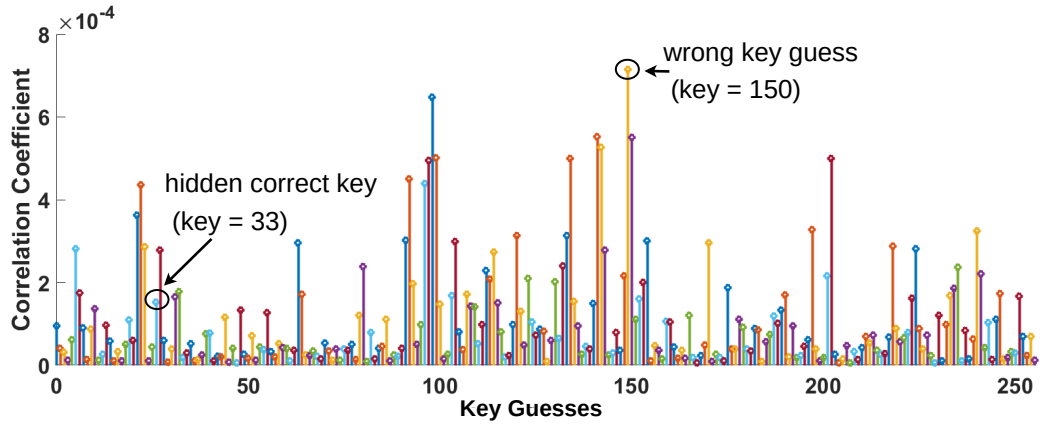



Figure 3.12: A non-successful DPA attack on S-box circuit implemented using the proposed EE-SPFAL gates with key=33.

value is peak for key guess=33. The correlation coefficient value for the correct key is 0.7. The correlation coefficient value for EE-SPFAL S-box circuit is maximum for key guess=150. The correlation coefficient of the hidden correct key (key=33) is $1.8X10^{-4}$. Figure 3.12 shows that the correct key is hidden when the DPA attack is performed on the EE-SPFAL based S-box circuit. We have also performed our test with another key. This time, we have chosen our key as $(181)_{10}$. It is shown that the CMOS based S-box circuit reveals the key as shown in Figure 3.13 and the correct key is hidden in EE-SPFAL based S-box circuit (Figure 3.14). It is observed that the correlation coefficient of the EE-SPFAL based S-box circuit are very low (in order of $10^{-4}$) and have SNR value close to unity. SNR value close to unity indicates that the EE-SPFAL based S-box circuits are more secure than the CMOS based S-box circuit.

### 3.4.3 Analysis of the EE-SPFAL based S-box circuit

In this section, analysis of the EE-SPFAL based S-box circuit is done. Since the EE-SPFAL based gates are proposed for building DPA-resistant hardware in IoT based devices, security and energy efficiency becomes the major criteria for evaluation. The proposed EE-SPFAL logic uses four phase trapezoidal clocks to recover the charge stored in the load capacitors. Since we are targeting to implement DPA-resistant hardware in IoT based devices,

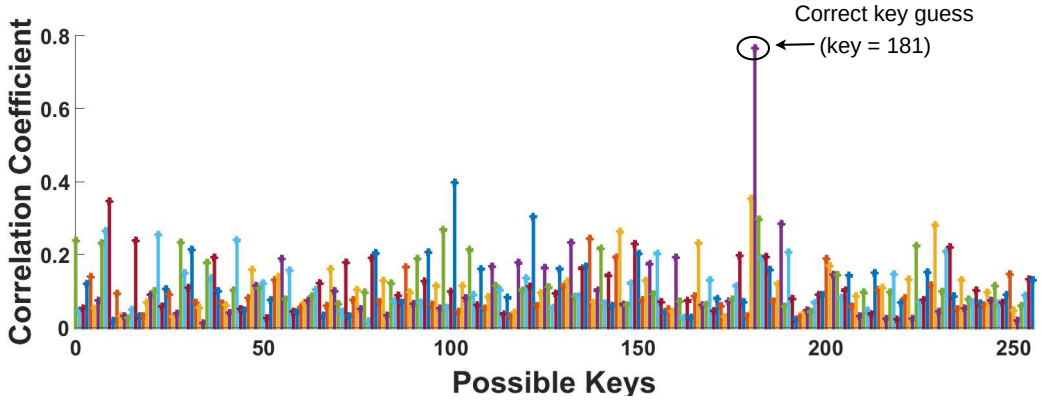



Figure 3.13: A successful DPA attack on S-box circuit implemented using CMOS implementation with key=181.

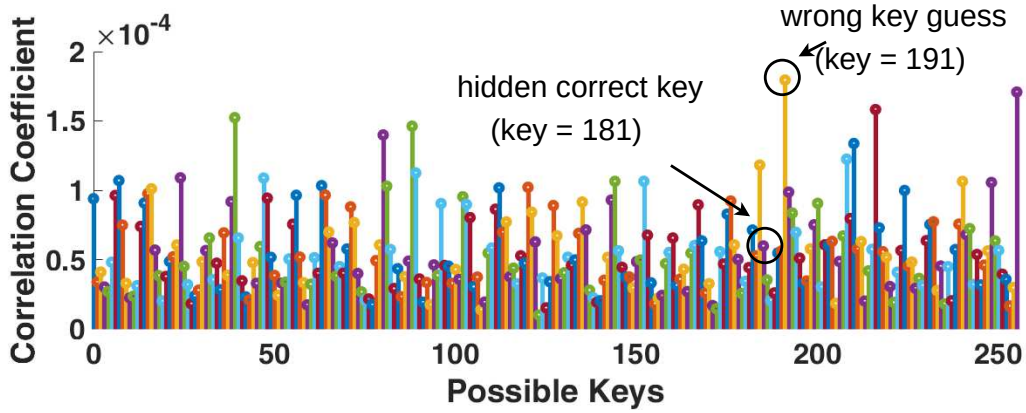



Figure 3.14: A non-successful DPA attack on S-box circuit implemented using the proposed EE-SPFAL gates with key=181.

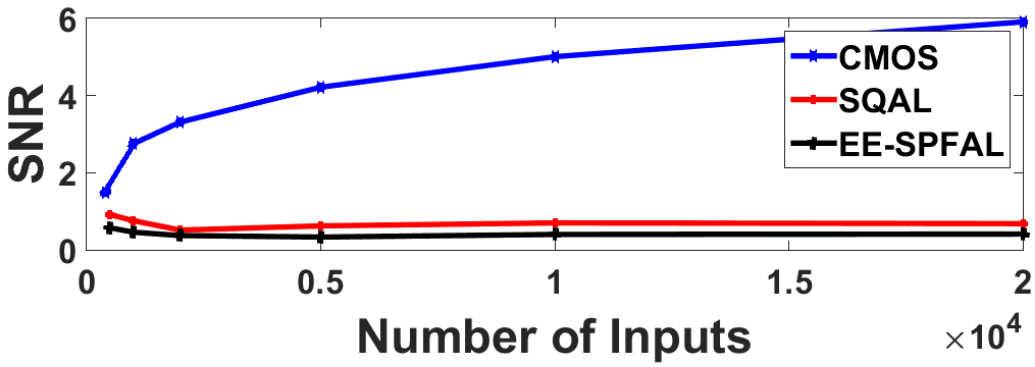



Figure 3.15: SNR values of CMOS, SQAL, and EE-SPFAL.

we want to use less number of voltage sources as compared to the existing DPA-resistant adiabatic logic families. For example, CSSAL based logic requires twelve trapezoidal voltage sources to implement the complex logic structure. An increase in the number of voltage sources increases the area of the chip and the power consumption. Among all of the DPA-resistant adiabatic logic proposed so far, SQAL logic seems to be optimized in terms of energy efficiency and area. Thus, we are comparing the transistor count and the energy dissipated per cycle of EE-SPFAL based S-box circuit with the SQAL logic based S-box circuit. Table 3.6 gives the comparison results of the EE-SPFAL, SQAL and CMOS based S-box circuit. Energy Saving Factor (ESF) is a measure of how much energy is used in the conventional CMOS gate or system with respect to its adiabatic logic counterpart [72].

**Area analysis of EE-SPFAL based S-box circuit**

We have implemented EE-SPFAL, SQAL, and CMOS based S-box circuit in Cadence Virtuoso using $180nm$ technology and simulated using Spectre simulator at nominal conditions. The length and width of all the transistors in the designs are $180nm$ and $2\mu m$ respectively. The total number of transistors used to implement the EE-SPFAL, SQAL and CMOS based S-box circuit is 4458, 3401, 2202 transistors respectively. It can be seen from the Table 3.6 that the EE-SPFAL based S-box circuit has the area overhead of 102.4% as compared to the CMOS based S-box circuit and 31.07% as compared to the SQAL based

S-box circuit.

Table 3.6: Implementation results of PPRM based S-box circuit using conventional CMOS, SQAL, and EE-SPFAL logic.

| Logic | No. of transistors (S-box) | Area ($mm^2$) | Energy dissipation | Energy Saving Factor |
|---|---|---|---|---|
| Conventional CMOS | 2202 | 0.04 | 33.5 nJ | - |
| SQAL [9] | 3401 | 0.0723 | 7.4 nJ | 4.54 |
| EE-SPFAL (Proposed) | 4458 | 0.092 | 2.638 nJ | 12.5 |

**Security analysis of EE-SPFAL based S-box circuit**

The immunity of the EE-SPFAL adiabatic logic against DPA attacks is validated by calculating the signal-to-noise ratio (SNR) for various input samples. Signal-to-noise ratio is defined as the ratio between the correlation value of the correct key and the second maximal value of the wrong key guess [49]. Low SNR values show the difficulty in distinguishing the correct key and the wrong key. In this work we have run simulations for multiple random input samples from 500 to 20000 input samples. Note that for the EE-SPFAL based S-box circuit, for the wrong key guess (key=150), the correlation was close to $6.8X10^{-4}$ and was slightly higher than the second maximal correlation $6.4X10^{-4}$ leading to SNR value of 1.0625, which is close to unity. Figure 3.15 shows the SNR values of EE-SPFAL, SQAL and CMOS for various input samples. It shows that the SNR value of the EE-SPFAL topology is less when compared to SQAL topology. Low SNR values of the proposed EE-SPFAL adiabatic logic shows that EE-SPFAL based adiabatic logic is more secure than the existing DPA-resistant adiabatic logic families.

**Energy-efficiency analysis of EE-SPFAL based S-box circuit**

The EE-SPFAL based S-box circuit dissipates 2.638nJ of energy per cycle, the SQAL based S-box circuit dissipates 7.4nJ, and the CMOS based S-box circuit dissipates 33.5nJ of en-

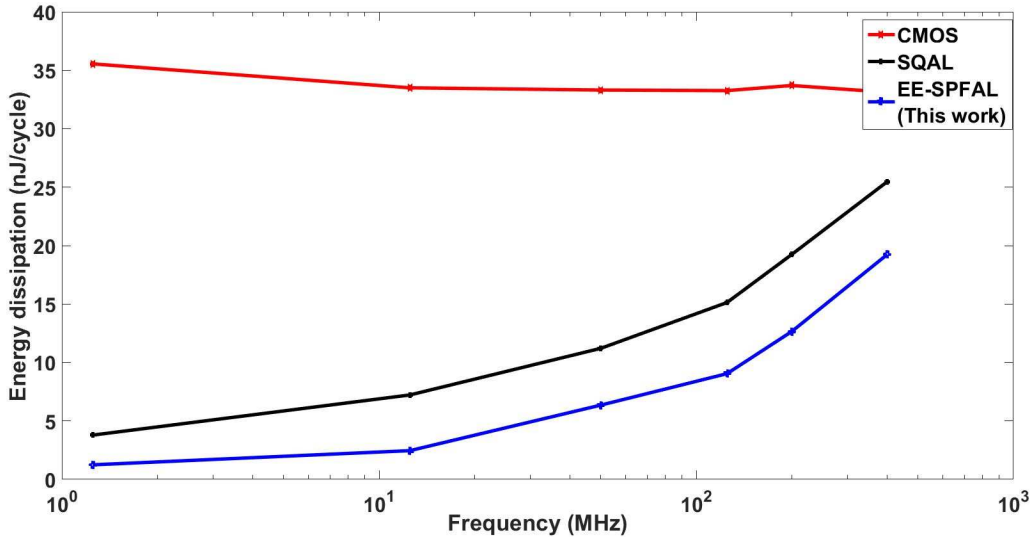



Figure 3.16: Energy dissipation comparison of S-box circuit implemented using CMOS, SQAL, and EE-SPFAL gates at different frequencies.

ergy per cycle at 12.5 MHz. Though the EE-SPFAL based S-box circuit has area overhead as compared to the SQAL logic and CMOS based logic, it saves about 65% of total energy dissipated per cycle and 90% of total energy dissipated per cycle of the SQAL and CMOS based S-box circuit. Figure 3.16 shows the comparison of the energy dissipated per cycle in the S-box circuits implemented using EE-SPFAL, SQAL and CMOS logic. We have performed the simulations at different frequencies to verify the functionality of the proposed S-box circuit. Simulations have been performed from 1.25 MHz to 125 MHz. It can be seen from the Figure 3.16 that as frequency increases, energy dissipation of the SQAL and EE-SPFAL based S-box circuit approaches the CMOS based S-box circuit. For the various frequency ranges, it can be seen that the energy dissipation of EE-SPFAL and SQAL differs by a constant energy dissipation (non-adiabatic energy loss) per cycle.

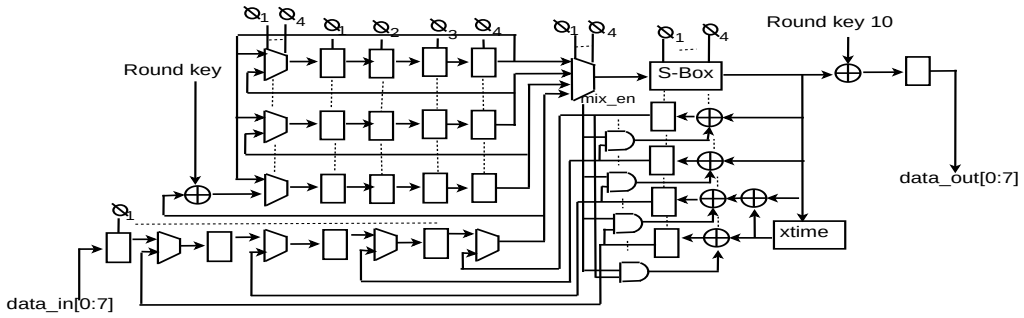



Figure 3.17: Implementation of an 8-bit AES encryption circuit [25].

### 3.4.4 Implementation of an AES encryption round using EE-SPFAL logic

In this research, we have implemented the first round of the AES algorithm [61] using EE-SPFAL gates. Figure 3.17 shows the 8-bit data path AES architecture with the on-fly key expansion unit as presented in [25]. In this architecture, round transformations are performed byte-by-byte as shown in the Figure. In the 8-bit AES architecture, shift row operations are modified in such a way that the 128-bit data is broken into 4 four-byte groups. The output of the shift row module is selected by a 4-to-1 multiplexer. Mix column is a byte oriented operation. In this work, we have performed the multiplication operation in the mix column using the Galois field multiplier [85]. In this architecture, all the blocks are designed using EE-SPFAL gates. The clocks are synchronized in each stage of the design. Additional buffers are inserted in order to synchronize the clocks. We make sure that the data is synchronized and fed to the corresponding blocks without any timing violations. In this design, we have used buffers instead of registers to store data for each clock. Each bit of the data is shifted after every clock cycle. However, in this architecture the data is fed each block in a sequential manner which leads to high delay in the output of the AES encryption circuit.

Round 0 of an AES algorithm consists of Add Round Key operation which is an XOR operation. Round 1 consists of S-box (Substitute Bytes), Shift Rows, Mix columns and Add Round Key operations. We have implemented round 0 and round 1 of the AES algorithm.

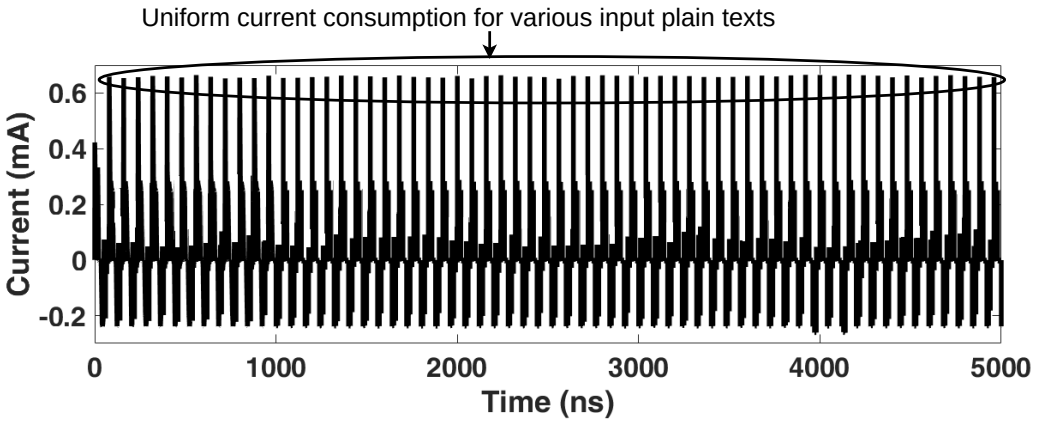



Figure 3.18: Uniform current consumption of the test circuit (Add Round Key and S-box circuit) implemented using EE-SPFAL logic.

It has to be noted that in 128-bit encryption AES algorithm, round 1 is repeated 9 times to encrypt the data. So, in this research, we are considering the power consumption of the single round of the AES algorithm as the other rounds consume the same amount of power as the first round except for the last round. Since EE-SPFAL logic counteracts DPA attacks at circuit level, it is expected that any complex algorithm implemented using EE-SPFAL logic will consume uniform current irrespective of the data being processed. As an illustrative example, we have shown the current consumption of round 1 of the AES algorithm. From the simulation results, we can see that the test circuit (Add Round Key and S-box) consumes uniform current of 0.68 mA (Figure 3.18) and AES round 1 implemented using EE-SPFAL logic consumes uniform current of 4.2 mA (SPICE simulation result) irrespective of data being processed as shown in Figure 3.19.

### 3.4.5 Summary

We have proposed a novel DPA-resistant adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL). Non-adiabatic energy loss is dominant in adiabatic circuits for low speed circuits. EE-SPFAL reduces the non-adiabatic energy loss by proper switching of the transistor such that whenever a transistor turns ON, there is no potential difference between the two operating nodes. Further, EE-SPFAL is se-

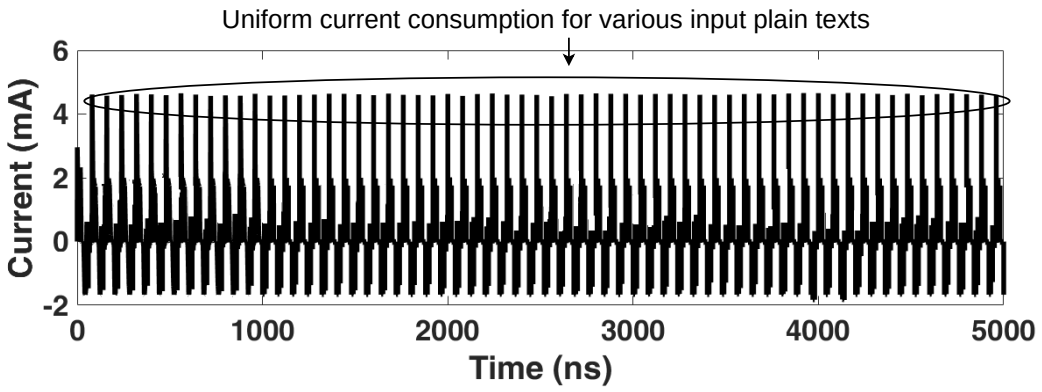



Figure 3.19: Uniform current consumption of AES round 1 implemented using EE-SPFAL logic.

cure against DPA as it breaks the correlation between the power consumption and the data processed. The security of EE-SPFAL against DPA attacks is validated by implementing a AES S-box circuit and performing DPA attacks through SPICE simulations. As EE-SPFAL is energy-efficient and secure against DPA attacks, the cryptographic circuits based on it can be employed in IoT based portable electronic devices.

# Chapter 4

# FinSAL: FinFET Based Secure Adiabatic Logic

Along with the low-power circuit design methodologies, various low-leakage emerging devices has been investigated to address the power budget issue in IoT devices. Among the various devices, FinFET devices are widely adopted by industries for the design of low power IoT nodes. FinFET has advantages such as higher on-state current, higher switching speed and low-leakage. So, in this chapter, we have investigated the usefulness of FinFET device along with adiabatic logic and we have proposed a novel FinFET based Secure Adiabatic Logic (FinSAL) to address the power budget and DPA attack problem in IoT devices.

## 4.1 FinFET device

FinFET has a three dimensional structure which has a thin silicon body perpendicular to the plane of the wafer. The channel of the FinFET is wrapped by the gate in all three directions. Figure 4.1(a) shows the three dimensional structure of the FinFET device. FinFET provides strong gate control over channels. Strong gate control over channels reduces the short-channel effects, threshold current, and gate-dielectric leakage current compared

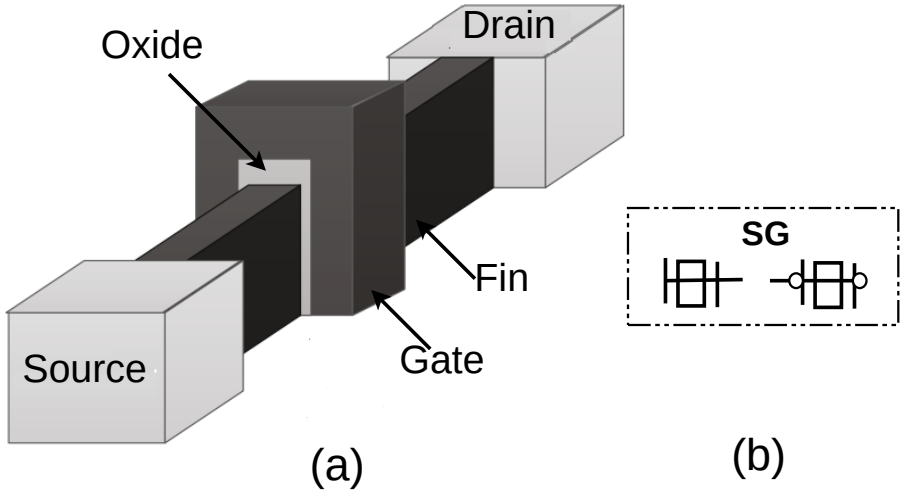



Figure 4.1: (a) Three dimensional structure of SG mode FinFET, (b) Symbols of SG mode FinFET.

to MOSFETs [28]. Better gate control in FinFETs over MOSFETs results in higher on-state current, lower leakage, and faster switching speed. Multi-gate structure of FinFET allows for different working modes of FinFET. The two main working modes for FinFET are Shorted-Gate (SG) mode and Independent-Gate (IG) mode.

### 4.1.1 Shorted-Gate (SG) mode

In the Shorted Gate (SG) mode, double gate (back gate and front gate) of the FinFET are tied together. FinFET acts as a three terminal device in SG mode. Figure 4.1(b) shows the symbols of SG mode FinFET.

### 4.1.2 Independent-Gate (IG) mode

In the Independent Gate (IG) mode, top part of the gate is removed to form two independent gates. The front gate and back gate are connected to two different inputs. FinFET acts as a four terminal device in IG mode. The special case of IG mode to reduce the threshold leakage is called as Low-Power (LP) mode.

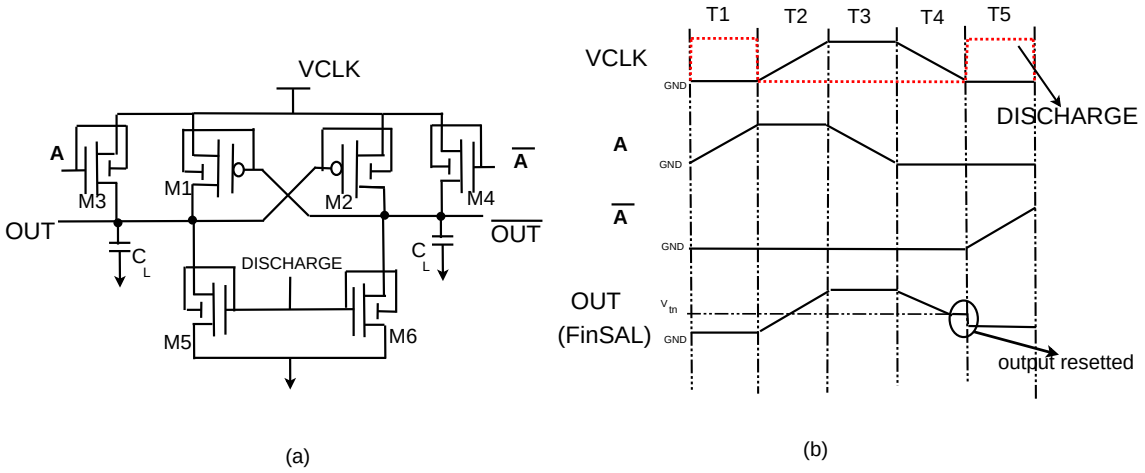



Figure 4.2: a) Schematic diagram of FinSAL buffer, b) Timing diagram for FinSAL buffer.

## 4.2 Logic structure of FinSAL gates

This section explains the logic structure of proposed FinFET based Secure Adiabatic Logic (FinSAL). In this research, we have investigated the FinSAL in SG mode type. SG mode can be considered a replacement to bulk CMOS without changing the configuration of existing circuits.

The proposed FinFET based Secure Adiabatic Logic (FinSAL) buffer is depicted in Figure 4.2(a). Input and output signals shown in Figure 4.2(b) demonstrate the logic operation.

The working of the FinSAL buffer is explained through different phases of the clock (wait, evaluate, hold, recovery).

#### T1 (Wait phase)

In this phase, the power clock VCLK is stable at GND (low level). The evaluation path signal is established by **A** or $\overline{A}$ (M3 or M4) (Figure 4.2(a)). In this case (Figure 4.2(b)), **A** slowly rises from 0 to $V_{dd}$ which leads M3 to turn ON. The DISCHARGE signal is high ($V_{dd}$) in this phase to discharge the load capacitances through M5 or M6. The redundant charge stored in load capacitances are discharged to GND before the logic function is eval-

uated. Discharging the load capacitors before the evaluation of logic function prevents the circuit from depending on previous input data.

**T2 (Evaluate phase)**

In this phase, DISCHARGE signal is stable at GND (low level) which turns OFF M5 or M6. The power clock slowly rises from 0 to $V_{dd}$ which leads to flow of current through the evaluate transistors (M3 or M4). In this case (Figure 4.2(b)), when VCLK rises from 0 to $V_{dd}$, and the current flow through M3 which leads to the output load capacitor (OUT) to be charged.

**T3 (Hold phase)**

During the hold phase, the current active input signal is slowly decreased to low level (GND). The power clock VCLK is stable at high level ($V_{dd}$). The output signal remains stable in this phase. In this case (Figure 4.2(b)), **A** slowly decreases from $V_{dd}$ to 0. The OUT is stable at high level ($V_{dd}$).

**T4 (Recovery phase)**

During the recovery phase, the power clock VCLK slowly decreases from $V_{dd}$ to 0. The current active output discharges to a low level through M1 or M2. The charge stored in the active output load capacitor is discharged to VCLK through M1 or M2. Consequently, charge recovery happens in every clock cycle (T1-T4). Recovering the charge in every clock cycle minimizes the energy lost. In this case (Figure 4.2(b)), charge stored in the output load capacitor (OUT) is recovered back to VCLK through M1.

Power clocks required for this circuit is generated by a dedicated circuit. Examples of such adiabatic clock generation circuitry are explained in [87].

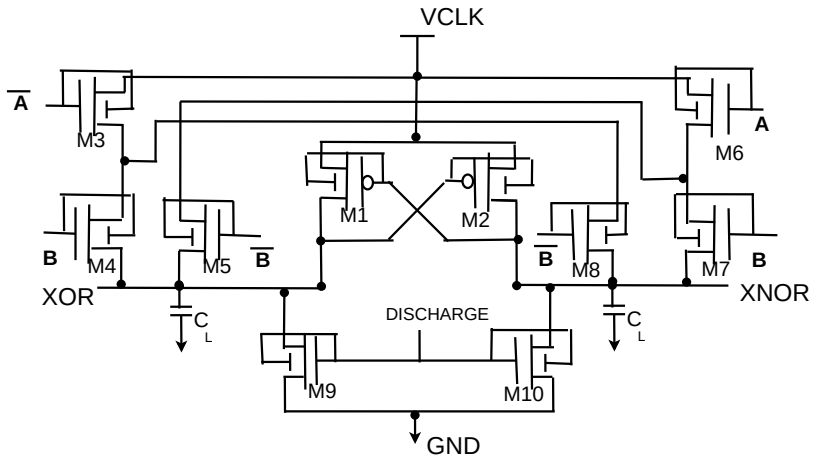



Figure 4.3: FinSAL XOR/XNOR gate.

## 4.3 FinSAL based logic gates

Figure 4.3 shows the schematic diagram of the FinSAL XOR/XNOR gate. In FinSAL XOR/XNOR gate, M1 and M2 transistors are used to recover the charge stored in the load capacitors to the power clock VCLK. M9 and M10 are used to discharge the redundant charge stored in the load capacitors before the evaluation of next phase inputs. Rest of the transistors are used for the evaluation of XOR/XNOR logic function. Figure 4.4 validates with an example of FinSAL XOR/XNOR gate that the proposed FinSAL gates have minimum output distortion which make them less vulnerable to DPA attack.

Figure 4.5 shows the schematic diagram of the FinSAL AND/NAND gate. In FinSAL AND/NAND gate, M1 and M2 transistors are used to recover the charge to the power clock VCLK. M13 and M14 are used to discharge the redundant charge stored in the load capacitors before the evaluation of next phase inputs. Rest of the transistors are used for the evaluation of AND/NAND logic function.

The intrinsic capacitance of the FinSAL based logic gates could play a critical role in the DPA resistance of the cryptographic circuits. This is because the unequal intrisic capacitances of the dual rail logic functions coupled with unbalanced load capacitances could produce non-uniform current consumption which can be easily observed through the

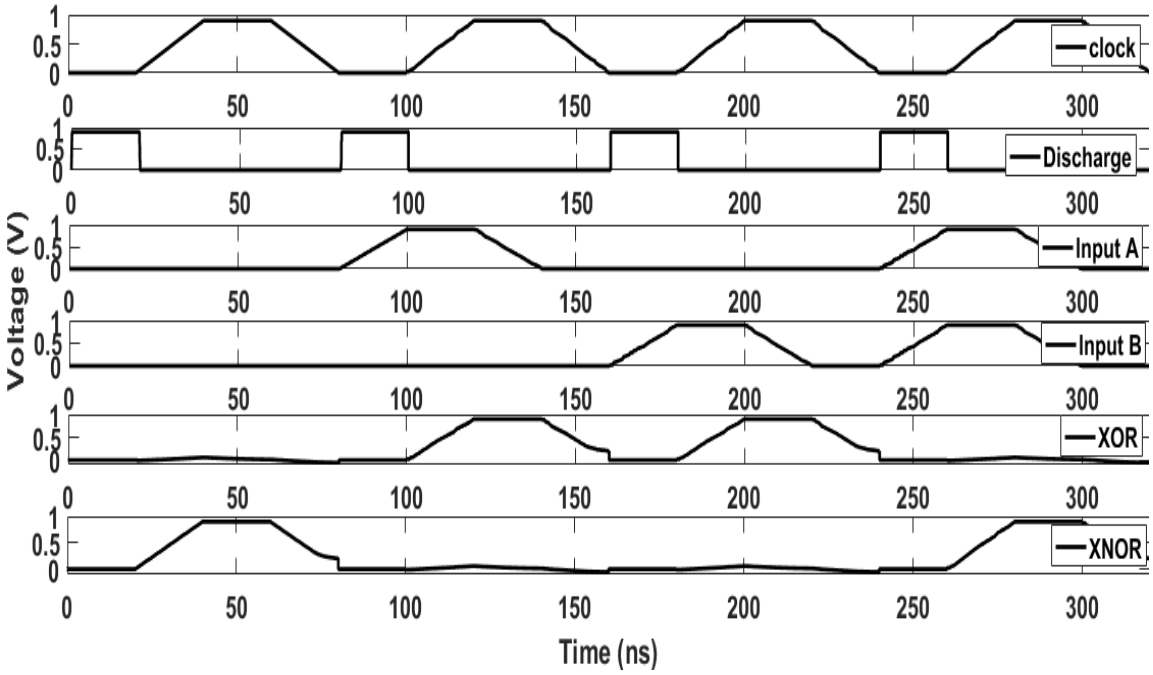



Figure 4.4: Input and output waveforms of FinSAL XOR gate.

output waveform. In this work, the security of the FinSAL based circuits are ensured by balancing the current consumption of the FinSAL based logic gates through proper gate sizing and manual layout of the circuit nodes. Current consumption in FinSAL based logic gates are balanced by balancing the load capacitances of the logic gates. For instance, the load capacitance of the FinSAL XOR/XNOR gate is balanced. The pull up network of the XOR logic function consists of two series transistors (M3 and M4) and a parallel transistor (M5). Similarly, the pull up network of the XNOR logic function consists of two series transistors (M6 and M7) and a parallel transistor (M8). Thus, the load capacitance of the FinSAL XOR/XNOR gate is balanced. The pull up network of the AND logic function can be designed by connecting the M3 and M4 transistors in series. Similarly, the pull up network of the NAND logic function can be designed by connecting the M8 and M10 transistors in parallel. But, the overall load capacitance of the AND logic function is not same as the overall load capacitance of the NAND logic function. In order to balance the load capacitance, M5, M6, M7 and M9 transistors are added. These transistors are

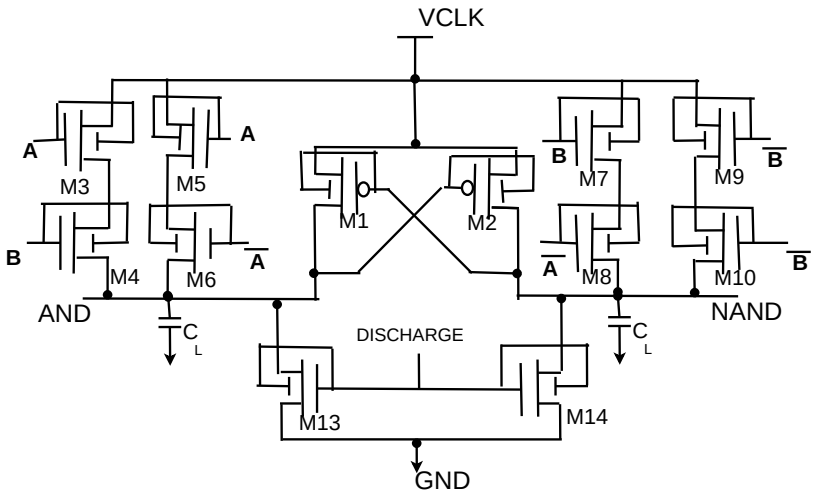



Figure 4.5: FinSAL AND/NAND gate.

connected in such a way (as shown in Figure 4.5) that the overall load capacitances of the AND and NAND logic functions are balanced while the functionality of the circuit remains the same.

### 4.3.1 Current consumption of adiabatic FinSAL XOR gate and FinFET based conventional XOR gate

Figure 4.6 shows the current consumed by the FinFET based conventional XOR gate with the load capacitor of 1fF. The current consumption of the FinFET based conventional XOR gate is not uniform. This can make the circuit vulnerable to DPA attack. Figure 4.7(a) shows the current consumed by the FinSAL XOR gate with equal size FinFETs. With equal size FinFETs, for each input transition peak current consumed by the FinSAL XOR gate is uniform. However, the current consumed during the hold phase of the clock is not uniform (Figure 4.7(a)). This non-uniform current consumption during the hold phase of the clock can make the circuit vulnerable to DPA attack.

To remove the DPA vulnerability during hold phase of the FinSAL gates, proper sizing of FinFETs are needed. Therefore, in FinSAL logic gates, discharging transistors are sized 2X that of the other FinFETs. Doubling the size of the discharge FinFETs balance the

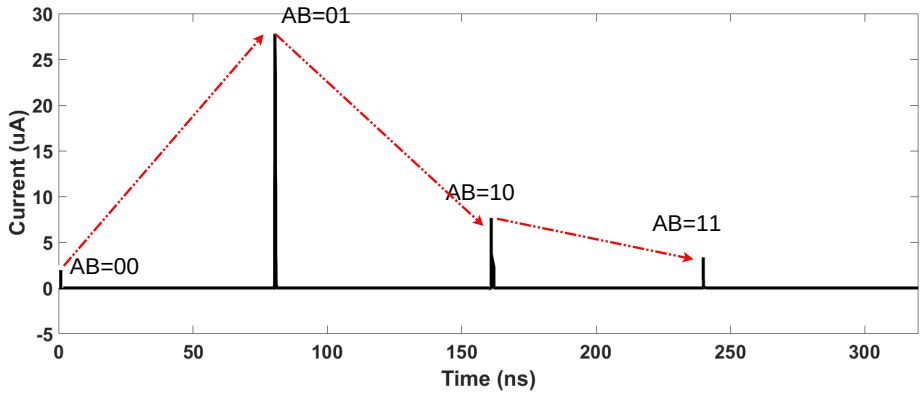



Figure 4.6: Current consumption of conventional XOR gate implemented in FinFET technology.

load capacitances. FinFETs have higher intrinsic capacitance than the MOSFET at same technology node. So, increase in the size of the discharge transistors helps to discharge the redundant charge before the evaluation of next cycle. Figure 4.7(b) shows the uniform current consumption of the FinSAL XOR with properly sized FinFETs. With doubling the size of the discharge FinFETs, current-data dependency at the hold phase is eliminated.

### 4.3.2 Energy consumption of FinSAL XOR gate

Figure 4.8 shows the energy consumed during each cycle of the adiabatic FinSAL and FinFET based conventional XOR gate. It can be seen that the FinFET based conventional XOR gate suffers from dynamic switching energy loss whenever there is a input transition. In the proposed adiabatic FinSAL XOR gate, there is a small energy loss during the reset of outputs. But the proposed adiabatic FinSAL XOR gate consumes less energy as compared to the FinFET based conventional XOR gate due to recovery of charge in each phase of clock cycle.

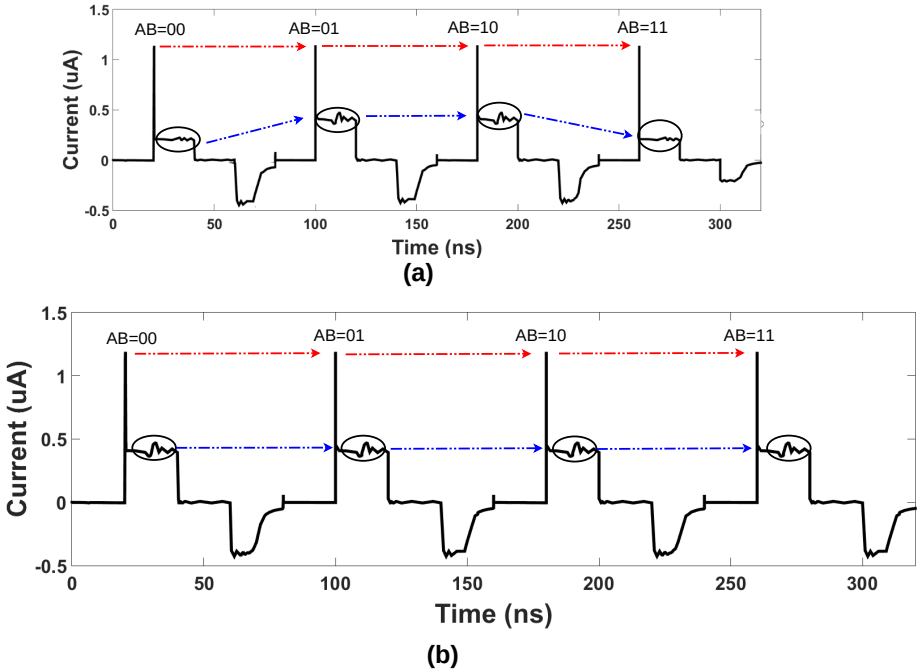



Figure 4.7: Current consumption of proposed FinSAL XOR gate for various input transitions with (a) all FinFETs are equally sized, (b) 2X effective width of discharge FinFETs.

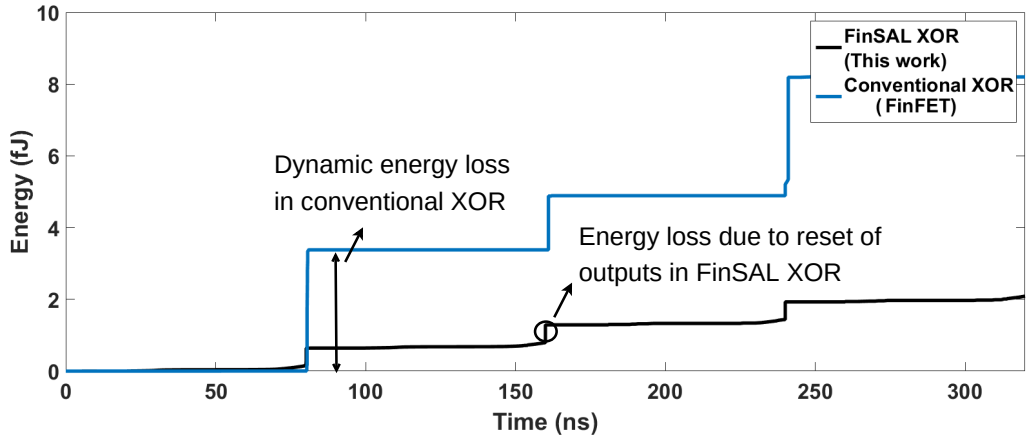



Figure 4.8: Energy consumption comparison between FinSAL and conventional FinFET based XOR gates.

## 4.4 Simulation result of FinSAL based logic gates ($20nm$ FinFET)

In this section, we present the simulation results of the proposed FinSAL based logic gates. The simulations are done in Cadence Virtuoso using Spectre simulator. Simulations are based on Predictive Technology Model (PTM) for $20nm$ FinFETs with the load capacitance of 1fF. Table 4.1 provides the $20nm$ FinFET technology parameters which are used for simulation. In the proposed designs, the size of the FinFETs are chosen to be minimum. Effective width in FinFETs is defined as $2 \times H_{fin} + t_{fin}$. So, for $20nm$ FinSAL gates, effective width of FinFETs of M1, M2, M3, and M4 in Figure 4.2(a) is $71nm$ and the effective length is $24nm$. However, the discharging FinFETs (M5 and M6 in Figure 4.2(a)) are sized 2X than the other FinFETs. In this case, the effective width of M5 and M6 are $142nm$. We have increased the size of the discharge FinFETs to discharge the redundant charge to ground. Increasing the effective width of FinFETs will allow more current to flow through the FinFETs. So, increasing the width of discharge FinFETs will discharge all the redundant charge to ground. *One key difference between the design of adiabatic CMOS and adiabatic FinFET for security application is that in adiabatic CMOS circuits all the transistors are sized equally while in adiabatic FinFET circuits, size of FinFETs need to be chosen carefully to achieve the uniform current profile irrespective of input transitions.*

Table 4.1: $20nm$ FinFET device parameters.

| | |
|---|---|
| Technology node | $20nm$ |
| Gate length ($L_g$) | $24nm$ |
| Fin height ($H_{fin}$) | $28nm$ |
| Fin width ($W_{width}$) | $15nm$ |
| Oxide thickness ($t_{ox}$) | $1.4nm$ |
| $V_{DD}$ | 0.9V |

The parameter Normalized Energy Deviation (NED), defined as $(E_{max} - E_{min})/E_{max}$, is used to indicate the percentage difference between minimum and maximum energy consumption for all possible input transitions. Normalized Standard Deviation (NSD) [15]

indicates the energy consumption variation based on the inputs and it is calculated as $\frac{\sigma_E}{\bar{E}}$. $\bar{E}$ denotes the average energy dissipation for various input transitions. In general, '$n$' input gate will have $2^{2n}$ possible input transitions. For example, 2 input gate will have 16 input transitions. $\sigma_E$ denotes the standard deviation of the energy consumed dissipated by the circuit and it is given by $\sqrt{\frac{\sum_{i=1}^{n}(E_i-\bar{E})^2}{n}}$. The calculated values of NED and NSD for the proposed FinSAL XOR gate and FinSAL AND gate show the ability of the FinSAL logic family to resist DPA attacks at cell level. Table 4.2 and Table 4.3 shows the simulated

Table 4.2: Simulated and calculated results for DPA-resistant adiabatic logic based XOR gate.

| Logic family | CSSAL [51] | SQAL [9] | FinSAL |
|---|---|---|---|
| Device | MOSFET | MOSFET | FinFET |
| Technology | $22nm$ | $22nm$ | $20nm$ |
| $E_{min}$(fJ) | 0.757 | 0.352 | 0.058 |
| $E_{max}$(fJ) | 0.957 | 0.707 | 0.06 |
| $E_{avg}$(fJ) | 0.865 | 0.515 | 0.059 |
| NED (%) | 0.15 | 0.502 | 0.002 |
| NSD(%) | 0.04 | 0.287 | 0.001 |

Table 4.3: Simulated and calculated results for DPA-resistant adiabatic logic based AND gate.

| Logic family | CSSAL [51] | SQAL [9] | FinSAL |
|---|---|---|---|
| Device | MOSFET | MOSFET | FinFET |
| Technology | $22nm$ | $22nm$ | $20nm$ |
| $E_{min}$(fJ) | 0.782 | 0.356 | 0.081 |
| $E_{max}$(fJ) | 0.972 | 0.706 | 0.094 |
| $E_{avg}$(fJ) | 0.865 | 0.492 | 0.088 |
| NED (%) | 0.15 | 0.495 | 0.093 |
| NSD(%) | 0.08 | 0.329 | 0.034 |

and calculated results of proposed FinSAL XOR and FinSAL AND gate respectively. The results of FinSAL gates are compared with Charge-Sharing Symmetric Adiabatic Logic (CSSAL) [51] and Secured Quasi-Adiabatic Logic (SQAL) [9]. From Table 4.2 and Table 4.3, it can be inferred that FinSAL based XOR and AND gate have very negligible energy

deviation for various input transitions. This property of FinSAL gates make them suitable to build DPA resistant hardware.

## 4.5 Reliability parameters of FinSAL logic against DPA attack

This section discusses the reliability parameter of FinSAL logic against DPA attack. In this section, we discuss the effect of change in load capacitances, number of fins and the clock on security of FinSAL logic.

### 4.5.1 Effect of load capacitance on security of FinSAL logic

The difference in load capacitance will result in difference in current consumption of the logic gates. Difference in current consumption due to the load capacitances result the circuit prone to DPA attack. So, balanced and unbalanced load test of proposed FinSAL based gates are performed in this research.

In the balanced test, we have chosen both the load capacitance values to be 1fF and we calculated the NED and NSD values. However, in practical circuits, due to manufacturing defects and routing issues, load capacitances of a gate may not be balanced. Unbalancing of the load capacitances reduce the reliability of the design in terms of security. In order to address the unbalanced load capacitance effect, we have tested our designs with unbalanced load with the tolerance in the capacitance value of 50%. In our case, one of the load capacitance is fixed to be 1fF and the other is 0.5fF. In FinSAL AND and XOR gates for balanced load capacitances, the number of observations and the energy dissipation chart shows the minimal deviation of energy consumptions. For FinSAL AND gate with balanced load capacitances, we can see that the minimum energy consumption of an AND gate is 0.081 fJ and maximum energy consumption of 0.094 fJ with a energy consumption difference of 0.013 fJ. The energy consumption range of energy deviations of a

FinSAL AND gate is very small which improves the security of these gates. In the worst case scenario, with an unbalanced load capacitances,FinSAL AND gate consumes minimum of 0.062 fJ and maximum energy consumption of 0.094 fJ. The range of the FinSAL AND gate with unbalanced load capacitance is 0.031 fJ. FinSAL AND gates with unbalanced gates has low energy deviations. This shows that routing problems in FinSAL based circuits when implementing complicated circuits won't affect the security of the circuits.

Further, we have performed the simulations with the unbalanced load capacitances. Results of FinSAL AND and FinSAL XOR gate with unbalanced load capacitances are presented in Table 4.4 and Table 4.5. It can be seen from Table 4.4 and Table 4.5 that for unbalanced load capacitances, FinSAL AND gate and FinSAL XOR gate have NED and NSD values less than 1%. Energy consumption, NED and NSD values of proposed FinSAL gates with balanced and unbalanced load capacitances show that FinSAL based logic gates can be used to design low-power, secure and miniaturized IoT devices.

Table 4.4: Simulated and calculated results for balanced and unbalanced FinSAL AND gates.

| Logic family | FinSAL (balanced) | FinSAL (unbalanced) |
|---|---|---|
| Technology | $20nm$ | $20nm$ |
| $E_{min}$(fJ) | 0.081 | 0.062 |
| $E_{max}$(fJ) | 0.094 | 0.094 |
| $E_{avg}$(fJ) | 0.088 | 0.081 |
| NED (%) | 0.133 | 0.342 |
| NSD(%) | 0.034 | 0.119 |

### 4.5.2 Effect of number of Fins on security of FinSAL logic

FinFETs have unique parameters compared to classical CMOS such as number of fins, thickness and height of fins. The thickness and the height of the fins are defined by the technology node, however the designer has the control over number of fins to improve the performance and the power characteristics of the design. Therefore, evaluation of FinSAL logic with respect to number of fins is performed. The size of the FinFET is defined by the

Table 4.5: Simulated and calculated results for balanced and unbalanced FinSAL XOR gates.

| Logic family | FinSAL (balanced) | FinSAL (unbalanced) |
|---|---|---|
| Technology | $20nm$ | $20nm$ |
| $E_{min}$(fJ) | 0.058 | 0.036 |
| $E_{max}$(fJ) | 0.06 | 0.06 |
| $E_{avg}$(fJ) | 0.059 | 0.043 |
| NED (%) | 0.02 | 0.274 |
| NSD(%) | 0.01 | 0.114 |

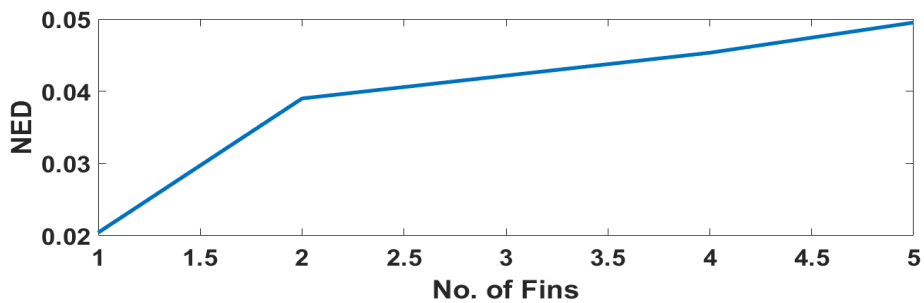



Figure 4.9: NED values as a function of number of fins in FinSAL XOR gate.

width and the length of the FinFET. The width of the FinFET is given by $n(2h_{fin} + t_{fin})$, where $h_{fin}$ is the height of the FinFET, $t_{fin}$ is the thickness of the FinFET and $n$ is the number of fins. Width of the FinFETs are quantized based on the number of fins. Higher value of width in FinFET is achieved by increasing the number of fins. Increasing the number of fins will allow more current to pass through the fins which results in higher on-current.

In this research, we have evaluated the effect of change in number of fins on security in FinSAL XOR gate. As an example, we have considered the effect of change in number of fins on the NED values. Figure 4.9 shows the variations of NED value with change in number of fins. With increase in the number of fins, it is observed that there is a slight increase in the NED values. With the increase in number of fins the current flow through the FinFETs increases which increase the NED values. Therefore, lower width FinFETs can provide better security compared to higher width FinFETs with the cost of decrease in

Table 4.6: Effect of clock jitter and clock delay with the security of FinSAL XOR gate.

| | without jitter | with jitter | with clock delay |
|---|---|---|---|
| $E_{min}$(fJ) | 0.058 | 217.6 | 105.4 |
| $E_{max}$(fJ) | 0.06 | 218.3 | 106.2 |
| $E_{avg}$(fJ) | 0.059 | 217.95 | 105.9 |
| NED (%) | 0.02 | 0.03 | 0.02 |
| NSD(%) | 0.01 | 0.01 | 0.01 |

performance.

### 4.5.3 Effect of clock on security of FinSAL logic

In FinSAL logic, four phase clocks are used to recover the energy from the load capacitors. However, delay in the clocks may lead to glitches which can affect the security of the FinSAL logic. As an example, we have performed the clock delay based simulations on a FinSAL XOR gate. Four FinSAL XOR gates are connected in series and the four phase clocks are applied with clock jitter and the second clock is delayed by 40ns. Table 4.6 shows the NED and NSD values of FinSAL XOR gate with jitter and clock delay. As expected, FinSAL XOR logic with clock jitter consume high power as compared to synchronized clock. However, FinSAL logic with jitter and clock delay has similar energy deviations compared to FinSAL logic without jitter. This shows that clock delay and clock jitter has minimum effect on security of FinSAL logic.

## 4.6 Evaluation of FinSAL logic gates at lower technology FinFET nodes

The main motivation of this section is to analyze the security offered by the FinSAL gates at lower FinFET technology nodes. With the lowering of FinFET technology, $V_{dd}$ is reduced. Reduction of power supply reduces the dynamic energy consumption. However, energy deviation of FinSAL gates at lower technology nodes can be found out by simulation based

experiments.

Security evaluation of the FinSAL logic gates are investigated at 16nm, 14nm, 10nm and 7nm FinFET technology nodes. As discussed earlier, NED and NSD values are considered as the security evaluation metrics for the logic gates. In order to consider the effect of routing issues and manufacturing defects, we have evaluated all the FinSAL logic gates with the balanced and unbalanced load capacitances. The unbalanced load capacitances are simulated with the tolerance of 50%.

Table 4.7: Comparison results of FinSAL AND gate at different FinFET technology nodes (balanced load capacitances).

| Technology | $20nm$ | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
|---|---|---|---|---|---|
| $E_{min}$(fJ) | 0.081 | 0.061 | 0.051 | 0.044 | 0.036 |
| $E_{max}$(fJ) | 0.094 | 0.07 | 0.057 | 0.05 | 0.039 |
| $E_{avg}$(fJ) | 0.088 | 0.066 | 0.055 | 0.047 | 0.037 |
| NED (%) | 0.133 | 0.125 | 0.106 | 0.103 | 0.086 |
| NSD(%) | 0.044 | 0.0411 | 0.0323 | 0.031 | 0.028 |

Table 4.8: Comparison results of FinSAL AND gate at different FinFET technology nodes (unbalanced load capacitances).

| Technology | $20nm$ | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
|---|---|---|---|---|---|
| $E_{min}$(fJ) | 0.062 | 0.046 | 0.037 | 0.032 | 0.025 |
| $E_{max}$(fJ) | 0.094 | 0.07 | 0.058 | 0.05 | 0.039 |
| $E_{avg}$(fJ) | 0.081 | 0.061 | 0.05 | 0.043 | 0.034 |
| NED (%) | 0.342 | 0.342 | 0.352 | 0.347 | 0.367 |
| NSD(%) | 0.119 | 0.12 | 0.126 | 0.123 | 0.132 |

Table 4.9: Comparison results of FinSAL XOR gate at different FinFET technology nodes (balanced load capacitances).

| Technology | $20nm$ | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
|---|---|---|---|---|---|
| $E_{min}$(fJ) | 0.058 | 0.045 | 0.0402 | 0.0354 | 0.0285 |
| $E_{max}$(fJ) | 0.06 | 0.048 | 0.0408 | 0.0359 | 0.0289 |
| $E_{avg}$(fJ) | 0.059 | 0.047 | 0.0405 | 0.0356 | 0.0287 |
| NED (%) | 0.02 | 0.064 | 0.0154 | 0.0152 | 0.0141 |
| NSD(%) | 0.01 | 0.033 | 0.007 | 0.007 | 0.007 |

Table 4.10: Comparison results of FinSAL XOR gate at different FinFET technology nodes (unbalanced load capacitances).

| Technology | $20nm$ | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
|---|---|---|---|---|---|
| $E_{min}$(fJ) | 0.036 | 0.028 | 0.024 | 0.021 | 0.017 |
| $E_{max}$(fJ) | 0.06 | 0.039 | 0.035 | 0.032 | 0.026 |
| $E_{avg}$(fJ) | 0.043 | 0.034 | 0.03 | 0.027 | 0.022 |
| NED (%) | 0.274 | 0.269 | 0.313 | 0.329 | 0.343 |
| NSD(%) | 0.114 | 0.114 | 0.142 | 0.152 | 0.161 |

### 4.6.1 FinSAL logic gates at $16nm$ technology FinFET nodes

Table 4.11: FinFET device parameters for different technology nodes.

| Technology node | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
|---|---|---|---|---|
| Gate length ($L_g$) | $20nm$ | $18nm$ | $14nm$ | $11nm$ |
| Fin height ($H_{fin}$) | $26nm$ | $23nm$ | $21nm$ | $18nm$ |
| Fin width ($W_{width}$) | $12nm$ | $10nm$ | $9nm$ | $7nm$ |
| Oxide thickness ($t_{ox}$) | $1.35nm$ | $1.3nm$ | $1.2nm$ | $1.15nm$ |
| $V_{DD}$ | 0.85V | 0.8V | 0.75V | 0.7V |

Table 4.11 shows the FinFET parameters which are used for the simulation of the FinSAL logic gates at lower technology nodes.

Table 4.7 and Table 4.9 show the comparison results of the FinSAL AND and FinSAL XOR gates at different technology nodes with the balanced load capacitances respectively. From Table 4.7 and Table 4.9, it can be inferred that $16nm$ FinSAL AND and FinSAL XOR gate with balanced load capacitances (0.8fF) consume 6% and 7% less energy as compared to the $20nm$ FinSAL AND and XOR gate. Table 4.7 and Table 4.9 also shows that $16nm$ FinSAL AND and XOR gate offer more resistant to DPA attacks with reduced NED and NSD values. Table 4.8 and 4.10 compare the results of the FinSAL AND and XOR gate at different technology nodes with the unbalanced load capacitances. From the simulation and calculated results, we have observed that $20nm$ FinSAL AND gate with unbalanced load capacitances offers security similar to $16nm$ FinSAL AND gate. Moreover, with FinSAL XOR gate, we have observed that $20nm$ FinSAL XOR gate offer better security than $16nm$ FinSAL XOR gate.

### 4.6.2 FinSAL logic gates at $14nm$ technology FinFET nodes

From Tables 4.7 and 4.9, it can be inferred that $14nm$ FinSAL AND and XOR gates with balanced load capacitances (0.7fF) consume 1% and 3% less energy as compared to the $16nm$ FinSAL gates. Though there is not significant improvement in energy consumption, $14nm$ FinSAL AND and XOR gate offers significant improvement in the security of the security gates with NED value less than 0.01%. Very minimum NED and NSD values of $14nm$ FinSAL AND and XOR gate makes it more secure as compared to the other technology FinSAL AND gate. However, $14nm$ FinSAL AND gate with unbalanced load capacitance (Table 4.8) offer similar security compared to other FinSAL AND gates. But, $14nm$ FinSAL XOR gate offers superior security as compared to other technology FinSAL XOR gate with unbalanced load capacitances (Table 4.10).

### 4.6.3 FinSAL logic gates at $10nm$ technology FinFET nodes

From Table 4.7 and Table 4.9, it can be inferred that $10nm$ FinSAL AND gate and FinSAL XOR gate with balanced load capacitances (0.6fF) consume 2% and 1% less energy as compared to the $14nm$ FinSAL AND and XOR gates. Though $10nm$ FinSAL AND gate has reduced energy consumption as compared to the $14nm$ FinSAL AND gate, it can be seen from Table 4.7 that $10nm$ FinSAL AND gate have higher NED values than $14nm$ FinSAL AND gate. Higher NED values results in reduction in security of the $10nm$ FinSAL AND gate than $14nm$ FinSAL AND gate. $10nm$ FinSAL XOR gate has almost same energy consumption and offers same security as $14nm$ FinSAL XOR gate. However, with the unbalanced load capacitances, $14nm$ FinSAL XOR gate offers superior security as compared to $10nm$ FinSAL XOR gate (Table 4.10).

### 4.6.4 FinSAL logic gates at $7nm$ technology FinFET nodes

With the lower technology nodes, $V_{dd}$ is reduced which results in the reduction of the energy consumption. From Table 4.7, it can be seen that $7nm$ FinSAL AND gate consumes less energy compared to all other FinSAL technology nodes. It is also shown that $7nm$ FinSAL AND gate with balanced capacitances (0.6fF) offer superior security as compared to $20nm$, $16nm$ and $10nm$ FinSAL logic gates. From our simulation results, we conclude that $14nm$ FinSAL AND gate offer superior security compared to all other FinSAL AND gate with balanced gates. However, $7nm$ FinSAL AND gate with unbalanced load capacitances offer similar security as $14nm$ FinSAL AND gate and consumes less energy compared to other FinSAL AND gate.

From Table 4.10, it can be infered that $7nm$ FinSAL XOR gate saves up to $1\%$ of energy compared to the FinSAL $10nm$ XOR gate. $7nm$ FinSAL XOR gate has almost same energy consumption and offers same level of security as $14nm$ FinSAL XOR gate. However, with the unbalanced load capacitances, $14nm$ FinSAL XOR gate offers superior security as compared to $7nm$ FinSAL XOR gate (Table 4.10).

## 4.7 Leakage power analysis of FinSAL logic gates

With the scaling of technology (sub 100nm), leakage power is known to be comparable to the dynamic power and is expected to become larger [20]. For IoT based devices, miniaturization is also an important aspect in the design along with the security and the battery power. Miniaturization is done by scling the device. In a recent article on effectiveness of leakage power analysis attacks on DPA-resistant logic styles by Alioto et. al, it has been proved that the existing DPA-resistant logic styles are unsecured, which means the leakage power can be used to reveal the secret keys [2].

FinFET is considered as a low-leakage emerging transistor which has very low leakage power compared to MOSFET due to the double gate control over the channel. In this sec-

tion, we are analyzing the reduction of leakage power in the adiabatic logic based FinSAL gates implemented at different FinFET technology nodes. In this work, leakage power is calculated during the hold phase of the clock.

### 4.7.1 Leakage Power Analysis of DPA Resistant AND gate

Table 4.12 provides the leakage power of various DPA resistant adiabatic logic families for a 2 input AND gate. We have calculated the leakage power of MOSFET device based DPA-resistant adiabatic logic families at $45nm$ technology. We have calculated leakage power at $45nm$ of MOSFET device because $45nm$ MOSFETs have significant leakage power as compared to $180nm$ MOSFET device [68].

Table 4.12: Leakage power of various DPA resistant adiabatic logic families at different technology for all possible inputs for a 2 input AND gate.

| Logic family | CSSAL [51] | SQAL [9] | FinSAL (This work) | | | | |
|---|---|---|---|---|---|---|---|
| Technology | $45nm$ | $45nm$ | $20nm$ | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
| Leakage power (A=0,B=0)(pW) | 201.6 | 129.8 | 38.3 | 38.5 | 36.09 | 42.3 | 42.01 |
| Leakage power (A=0,B=1)(pW) | 198.5 | 130.9 | 42.8 | 40.8 | 37.7 | 49.6 | 49.4 |
| Leakage power (A=1,B=0)(pW) | 187.4 | 154.08 | 46.3 | 43.9 | 44.03 | 46.49 | 46.8 |
| Leakage power (A=1,B=1)(pW) | 203.95 | 154.96 | 50.9 | 46.9 | 39.1 | 41.8 | 44.07 |
| Average Leakage power(pW) | 197.8 | 142.4 | 44.57 | 42.52 | 39.23 | 45.04 | 45.57 |

From Table 4.12, it is shown that MOSFET device based gates have higher leakage power as compared to the FinFET based gates. MOSFET devices have higher leakage power at lower technology nodes due to the formation of the leakage current in the short channel of the devices. However, leakage currents in the FinFETs can be reduced by the control of double gates. It is clear from the results shown in Table 4.12 that FinSAL AND gates reduces leakage power dissipation compared to the MOSFET based DPA-resistant adiabatic logic families.

$14nm$ FinSAL AND gate has very low leakage power as shown in Table 4.12. $14nm$ FinSAL AND gate has 80.1 % of reduction of leakage current as compared to CSSAL AND gate. $14nm$ FinSAL AND gate has also reduced leakage power as compared to other DPA-resistant adiabatic logic familes. For example, $14nm$ FinSAL AND has 72.45% reduction of leakage power as compared to SQAL AND gate. $14nm$ FinSAL AND gate has 11.9 %, 7.7 %, 12.8 % and 13.9 % reductions of leakage power as compared to the FinSAL AND gate implemented in $20nm$, $16nm$, $10nm$ and $7nm$ FinFET technologies respectively.

### 4.7.2 Leakage Power Analysis of DPA Resistant XOR gate

Table 4.13 shows the leakage power of the DPA resistant XOR gate simulated at 12.5 MHz. Similar to the DPA-resistant AND gate, MOSFET based DPA-resistant XOR gate have higher leakage power than the FinFET based gates. As expected FinSAL based XOR gate shows reduced leakage power consumption as compared to the other DPA-resistant adiabatic logic families. Similar to FinSAL AND gate, $14nm$ FinSAL XOR gate has lower leakage power consumption.

Table 4.13: Leakage power of various DPA resistant adiabatic logic families at different technology for all possible inputs for a 2 input XOR gate.

| Logic family | CSSAL [51] | SQAL [9] | FinSAL (This work) | | | | |
|---|---|---|---|---|---|---|---|
| Technology | $45nm$ | $45nm$ | $20nm$ | $16nm$ | $14nm$ | $10nm$ | $7nm$ |
| Leakage power (A=0,B=0)(pW) | 203.01 | 171.9 | 35.6 | 31.63 | 28.3 | 27.9 | 29.5 |
| Leakage power (A=0,B=1)(pW) | 190.50 | 172.4 | 35.7 | 31.79 | 27.7 | 30.6 | 29.7 |
| Leakage power (A=1,B=0)(pW) | 190.75 | 171.6 | 35.7 | 31.34 | 27.8 | 30.7 | 29.6 |
| Leakage power (A=1,B=1)(pW) | 202.30 | 173.61 | 35.8 | 31.78 | 27.8 | 31.2 | 29.7 |
| Average Leakage power(pW) | 196.64 | 172.3 | 35.7 | 31.63 | 27.9 | 30.1 | 31.625 |

$14nm$ FinSAL XOR gate has 85.8%, and 83.8% reduction in leakage current as compared to CSSAL, and SQAL XOR gates respectively. $14nm$ FinSAL XOR gate has also

reduced leakage power consumption as compared to FinSAL XOR gate implemented in other FinFET node technologies. As shown in Table 4.13, $14nm$ FinSAL XOR gate has 21.8%, 13.36 %, 7.3 % and 11.3% reduction in leakage power compared to the FinSAL XOR gate implemented in $20nm$, $16nm$, $10nm$ and $7nm$ FinFET technologies respectively.

## 4.8 Energy-efficiency and security evaluation of the FinSAL based S-box circuit

In order to evaluate the security of the proposed FinSAL logic, we have implemented a Positive Polarity Reed Muller (PPRM) architecture based S-box circuit [57] using FinSAL gates and performed Differential Power Analysis (DPA) attack on it. DPA attack is perfomed as described in chapter 2 of this proposal.

### 4.8.1 Test case for FinSAL based S-box circuit

In our test case, the key was chosen to be $(181)_{10}$. A DPA attack was performed on FinSAL based S-box circuit and FinFET based conventional S-box circuit. It was found that the DPA attack was successful on the FinFET based conventional S-box circuit with 512 random plain texts whereas the DPA attack performed on FinSAL based S-box circuit was unsuccessful. Figure 4.10 shows the correlation coefficient values of the hypothetical key guesses for the successful DPA attack in a conventional S-box circuit. It can be seen that the correlation co-efficient value is peak for key guess=181. The correlation coefficient value for the correct key is 0.78. Figure 4.11 shows the non-successful DPA attack performed on the 8-bit S-box circuit implemented using FinSAL gates. The correlation coefficient value is maximum for key guess=231. The correlation coefficient of the hidden correct key (key=181) is $1.6X10^{-4}$.

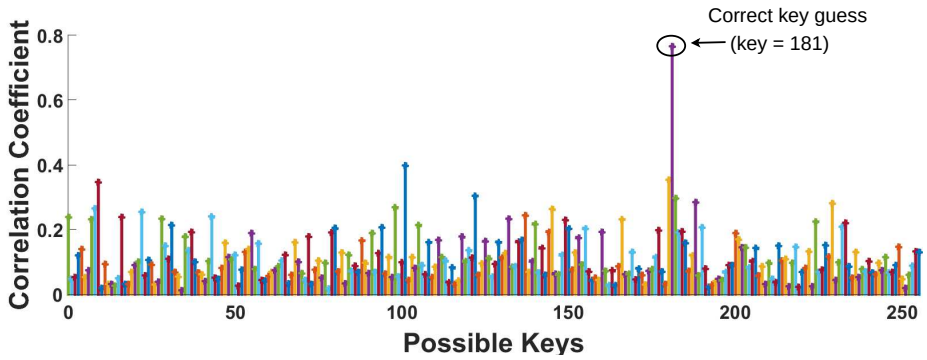



Figure 4.10: A successful DPA attack in a FinFET based conventional CMOS circuit.

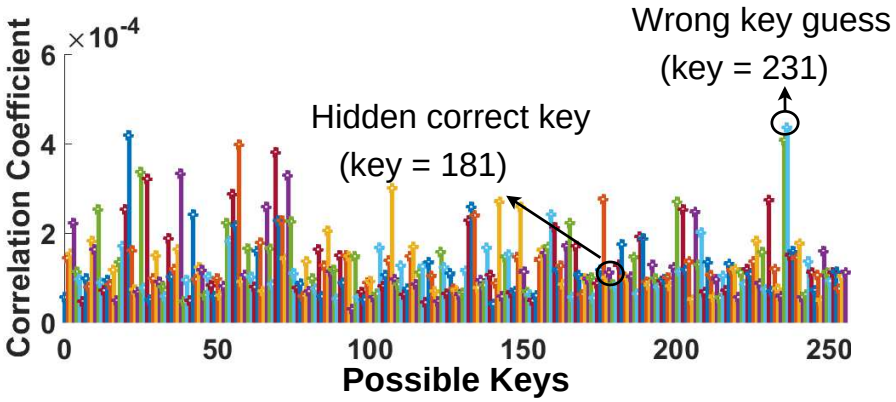



Figure 4.11: A non-successful DPA attack in a FinSAL based S-box circuit.

### 4.8.2 Analysis of FinSAL based S-box circuit

In this section, analysis of the FinSAL based S-box circuit is done. Since the FinSAL based gates are proposed for building DPA-resistant hardware in IoT based devices, security and energy efficiency becomes the major criteria of evaluation. The proposed FinSAL logic uses four phase trapezoidal clocks to recover the charge stored in the load capacitors. Since we are targeting to implement DPA-resistant hardware in IoT based devices, we are making sure to use a minimum number of voltage sources as compared to the existing DPA-resistant adiabatic logic families. The total number of FinFETs used to implement the FinSAL and conventional S-box circuit are 3624 and 2202, respectively. From our simulations, we found that the FinSAL S-box circuit works up to 800 MHz. However, from our simulations, we found that FinSAL S-box circuit is energy-efficient than its CMOS counterpart up to 400 MHz.

#### Security analysis of FinSAL S-box circuit

The immunity of the FinSAL logic against DPA attack is validated by calculating the Signal-to-Noise Ratio (SNR). Signal-to-Noise Ratio is defined as the ratio between the correlation value of the correct key and the second maximal value of the wrong key guess [49]. Low SNR values show the difficulty in distinguishing the correct key and the wrong key. For the FinSAL based S-box circuit, the wrong key guess (key=231) has the maximum correlation close to $4.35X10^{-4}$ and was slightly higher than the second maximal correlation $4.25X10^{-4}$ leading to SNR value of 1.023, which is close to unity. For the FinFET implementation of conventional CMOS based circuit, for the correct key guess, the correlation value was 0.8 and was much higher than the second maximal value 0.42 leading to SNR value of 1.904. SNR value of FinSAL S-box circuit close to unity shows that it is difficult to distinguish the correct key and the wrong key in a FinSAL S-box circuit.

Figure 4.12 shows the SNR values of the FinSAL logic at different FinFET technology nodes as a function of number of inputs. Figure 4.13 shows the SNR values of the Fin-

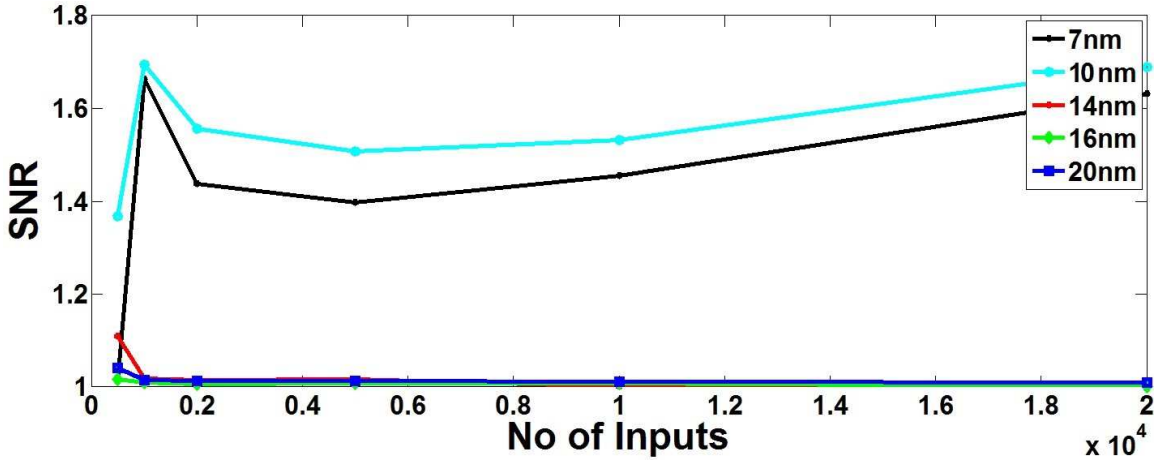



Figure 4.12: Signal-to-Noise ratio comparison of FinSAL logic at different FinFET technology nodes as a function of number of inputs.

SAL logic at different frequencies. SNR values for each technology node are calculated as a function number of inputs. In this research, we have passed up to 20,000 random input samples to the test circuit to calculate the SNR values with each technology nodes of FinSAL logic. We have observed that, FinSAL logic implemented with $14nm$ FinFET technologies have SNR value close to unity. SNR value near to unity shows that it is difficult to distinguish between the correct key and wrong key.

**Energy-efficiency analysis of FinSAL S-box circuit**

This section discusses the energy efficiency of the FinSAL S-box circuit as compared to the other DPA resistant adiabatic logic based S-box circuits. Table 4.14 gives the comparison results of the S-box circuit implemented with different DPA resistant adiabatic logic family. In this work, we are comparing the Energy Saving Factor (ESF) of the S-box circuit implemented with different DPA resistant adiabatic logic family. ESF is defined as a measure of how much energy is used in a conventional CMOS gate or system with respect to its adiabatic counterpart [72]. In this research, ESF values are calculated based on conventional CMOS S-box circuit implemented in $22nm$ MOSFET. As seen from Table 4.14, FinSAL S-box circuit implemented with 7nm FinFETs are more energy efficient with a ESF value of

Table 4.14: Comparison results of S-box circuit implemented with different adiabatic logic family at 12.5 MHz.

| Logic | Device | Technology node | No. of transistors (S-box) | Power Delay Product | ESF |
|---|---|---|---|---|---|
| Conventional CMOS | MOSFET | $22nm$ | 2202 | 1.5 pJ | - |
| CMOS | FinFET | $20nm$ | 2202 | 0.162 pJ | NA |
| CSSAL [52] | MOSFET | $22nm$ | 8115 | 0.76 pJ | 1.97 |
| SQAL [9] | MOSFET | $22nm$ | 3401 | 0.32 pJ | 4.687 |
| FinSAL | FinFET | 20nm | 3624 | 0.04 pJ | 37.5 |
| | FinFET | $16nm$ | 3624 | 0.034 pJ | 44.11 |
| | FinFET | $14nm$ | 3624 | 0.0258 pJ | 58.13 |
| | FinFET | $10nm$ | 3624 | 0.0242 pJ | 61.98 |
| | FinFET | $7nm$ | 3624 | 0.0233 pJ | 64.377 |

64.377. ESF value of 64.377 shows that the FinSAL S-box circuit implemented with 7nm FinFET saves up to 98% of energy as compared to conventional CMOS based S-box circuit implemented with $22nm$ MOSFET. With the lowering of technology, maximum swing of the power supply is reduced which reduces the overall energy dissipation. As seen from the Table 4.14, FinSAL S-box circuit when implemented with the lower technology FinFET node saves more energy as compared to the FinSAL S-box implemented at higher technology nodes. As far as the other DPA- resistant logic styles, CSSAL consume more power due to large number of transistors, SQAL consume more energy due to the non-adiabatic operation of transistors during the evaluate phase of the clock. Reduced energy dissipation in FinSAL logic as compared to the existing DPA-resistant adiabatic logic families makes it suitable to implement in DPA resistant IoT devices where there is tight constraint on size of the device, power consumption and security of the device.

It has been showed that FinSAL S-box circuit has reduced energy consumption as compared to the CMOS based S-box circuit implemented in FinFET. FinSAL S-box circuit implemented at $20nm$ FinFET technology saves up to 81% of energy as compared to the CMOS based S-box circuit implemented in FinFET ($20nm$). Energy consumption im-

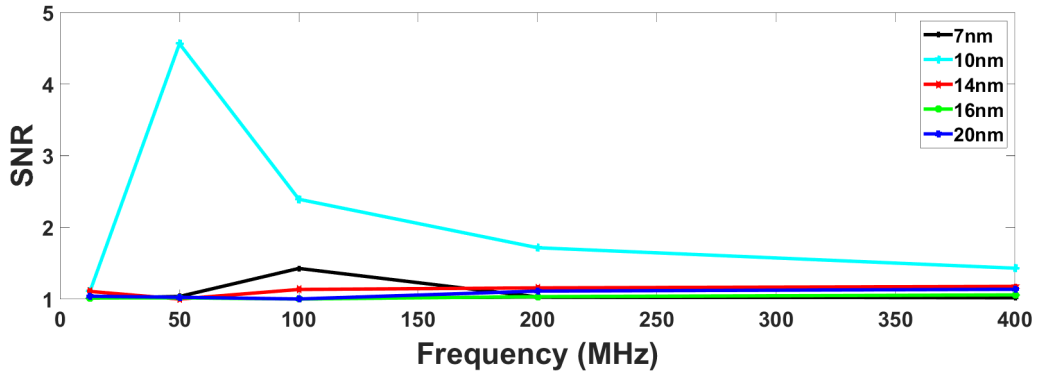



Figure 4.13: Signal-to-Noise ratio of FinSAL logic at different FinFET technology nodes as a function of operating frequency.

provement of FinSAL S-box circuit over CMOS based S-box circuit implemented in FinFET clearly shows that FinSAL gates are energy-efficient and can be used to implement in IoT devices.

## 4.9 Discussion

This section discusses about choosing the FinFET technology to design Energy-efficient and DPA-resistant IoT devices. From Table 4.14, it is shown that FinSAL logic is more energy-efficient as compared to the existing DPA-resistant adiabatic logic families. However, with the scaling of FinFET technology, security offered by the logic gates is changed. For example, $7nm$ FinFET technology have short channels as $14nm$ FinFET which increases the leakage current and makes the circuit more prone to DPA attack. But, $7nm$ FinFET technology is more energy-efficient as compared to the other technologies due to the reduction in the swing of the voltages. Reduction in the swing of the voltage sources reduces the dynamic energy consumption.

From Table 4.14, it is concluded that $7nm$ FinSAL logic is more energy-efficient as compared to the other FinSAL logics. However, Figure 4.12 shows that $7nm$ FinSAL logic is not secure as compared to other FinSAL logic. From the security perspective, we can see that $14nm$ FinFET technology offers superior security as compared to other FinSAL

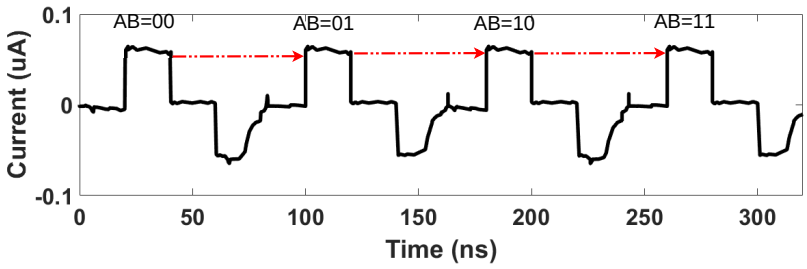



Figure 4.14: Current consumption of FinSAL XOR with trapezoidal discharge signal.

logic with a SNR value close to unity. Moreover, $14nm$ FinSAL logic has comparable energy consumption with $7nm$ FinSAL logic. From our simulation results, it is concluded that, FinSAL logic when implemented in $14nm$ FinFET technology nodes offer superior security and can be used to design secure IoT devices for future.

### 4.9.1 Minimization of huge current pulse in FinSAL logic

This section discusses about the methods to reduce of current pulse in FinSAL logic gates. The current consumption in FinSAL logic gates can be made uniform by proper sizing of FinFETs. However, FinSAL gates have huge current pulse (refer Figure 4.7) during the evaluate phase of the clock. This huge current pulse can be suppressed to make the FinSAL logic gates more secure against the DPA attack. We propose to reduce the huge current pulse by reducing the adiabatic energy loss. Energy consumption in adiabatic circuits can be reduced by increasing the transition period. So, one design technique which we can use to reduce the huge current pulse is by replacing the square wave discharge signal with the trapezoidal wave discharge signal. As an illustration, we have replaced the square wave discharge signal with the trapezoidal based discharge signal of FinSAL XOR gate. Figure 4.14 shows the current consumption of the FinSAL XOR gate with trapezoidal discharge signal.

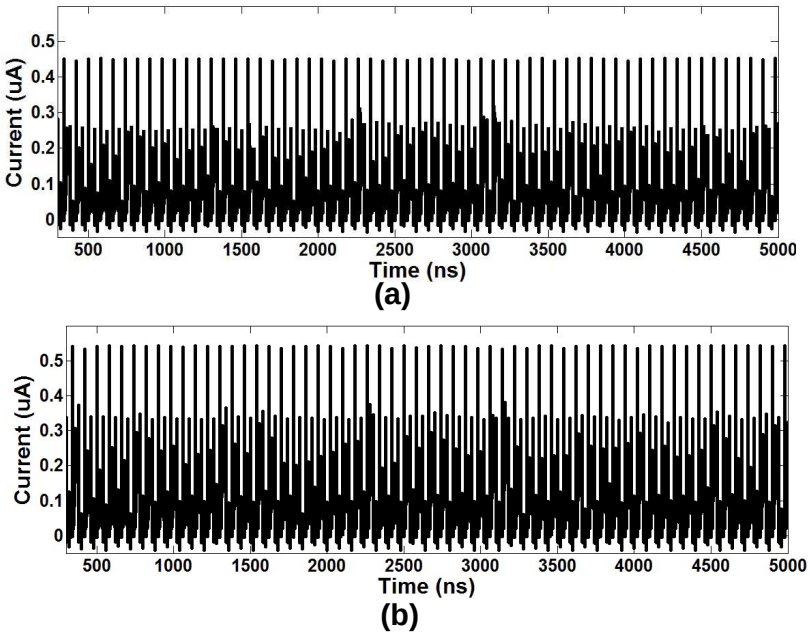



Figure 4.15: Current consumption of FinSAL S-box with number of fins a) n=1, (b) n=4. With n=1, the peak current consumption of FinSAL S-box is reduced approximately by 1.2 times than the FinSAL S-box circuit with n=4.

### 4.9.2 Impact of number of fins on FinSAL S-box circuit

The size of the FinFET is defined by the width and the length of the FinFET. The width of the FinFET is given by $n \times (2hfin + tfin)$, where hfin is the height of the FinFET, tfin is the thickness of the FinFET and n is the number of fins. Width of the FinFETs is quantized based on the number of fins. Higher value of width in FinFET is achieved by increasing the number of fins. Increasing the number of fins will allow more current to pass through the fins which results in higher on-current. Therefore, the performance of FinSAL based S-box circuit is evaluated by increasing the number of fins ($n$) with a case study of $n = 4$. Through SPICE simulation, it is validated that with $n = 4$ the peak current of FinSAL based S-box circuit is 1.2 times higher compared to the the peak current of FinSAL based S-box circuit with $n = 1$. Therefore, the performance of FinSAL based S-box circuit can be improved by increasing the number of fins (Figure 4.15). However, as illustrated for FinSAL XOR gate, the increase in number of fins reduces the security of FinSAL gates, therefore trade-off between performance and security need to be considered

while increasing the number of fins in adiabatic FinFET based cryptographic circuits.

## 4.10 Summary

In this chapter, we proposed a novel DPA-resistant adiabatic logic family called FinFET based Secure Adiabatic Logic (FinSAL). We have evaluated the security of the FinSAL logic to implement in secure IoT devices. At the gate level simulation of FinSAL logic, it is observed that change in number of fins has a significant effect on the security of the FinSAL logic gates. With the increase in the number of fins, security of FinSAL logic gate is reduced. However, the variations in $V_{dd}$ and the clock jitter do not have much impact on the security of the FinSAL logic gates. Further, the security of FinSAL against DPA attacks is validated by implementing a S-box circuit and performing DPA attacks through SPICE simulations. From our simulation results on FinSAL logic implemented at different technology nodes, it is concluded that FinSAL logic implemented at $14nm$ offers better security as compared to the other FinFET technology nodes. As FinSAL is energy-efficient and secure against DPA attacks, the cryptographic circuits based on it can be employed in IoT based portable electronic devices where there is a tight budget on power consumption and security.

# Chapter 5

# Exploration of Non-Volatile MTJ/CMOS Circuits for DPA Resistant Hardware

Recently, Magnetic Tunnel Junction (MTJ)/CMOS based Logic-in-Memory (LiM) circuits have been explored to design low-power non-volatile hardware. Some of the advantages of an MTJ device include non-volatility, near-zero leakage power, high integration density and easy compatibility with CMOS devices [22],[32],[33]. Hybrid MTJ/CMOS based Logic-in-Memory (LiM) architecture shows high potential in designing low power embedded hardware [90],[73]. However, the differences in power consumption between the change of spin orientations in MTJ devices increase the vulnerability to power analysis based side-channel attack. Further, the MTJ/CMOS hybrid logic circuits requiring frequent switching of spin orientations in MTJs are not very energy-efficient due to the significant energy required to switch the MTJ devices. In this chapter, we have investigated the novel approach of building cryptographic hardware in MTJ/CMOS circuits using Look-Up Table (LUT) based method where the data stored in MTJs are constant during the entire encryption/decryption operation..

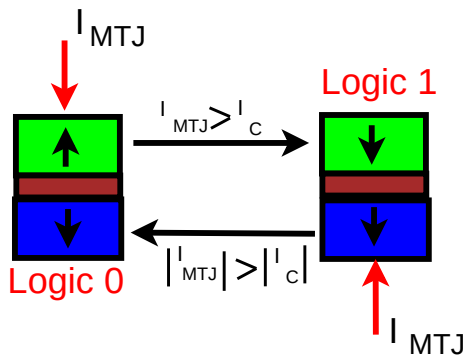



Figure 5.1: Magnetic Tunel Junction (MTJ) structure with Spin Transfer Torque (STT) switching mechanism where anti-parallel configuration represents logic 0 and parallel configuration represents logic 1.

## 5.1 Magnetic Tunnel Junction (MTJ)

Magnetic Tunnel Junction (MTJ) device mainly composed of an oxide barrier layer (e.g., MgO) sandwiched between two ferromagnetic layers (e.g., CoFeB) [53]. MTJ device can have two different resistance states depending on the relative magnetization of the FM layers. In general, the magnetization of one of the ferromagnetic layers is fixed, while the other ferromagnetic layer is free to take either parallel (P) and anti-parallel (AP) orientations as shown in Figure 5.1 [88]. Based on the ferromagnetic layer orientations, MTJ device will show either a low resistance (RP) or high resistance (RAP) characteristic [11]. The resistance difference between the two stable resistance states of MTJ device is given by the Tunnel Magnetoresistance ratio $TMR = (R_{AP} - R_P)/R_P$. From Figure 5.1, we can see that the anti-parallel configuration of MTJ can be represented as logic "0" and parallel configuration of MTJ can be represented as logic "1".

## 5.2 MTJ/CMOS circuits

Figure 5.2 shows the general structure of the existing MTJ/CMOS circuits. The Logic-in-Memory (LiM) architecture based MTJ/CMOS circuit consists of a Pre-Charged Sense Amplifier (PCSA) circuit, CMOS logic tree and MTJs. PCSA circuit is used for sensing

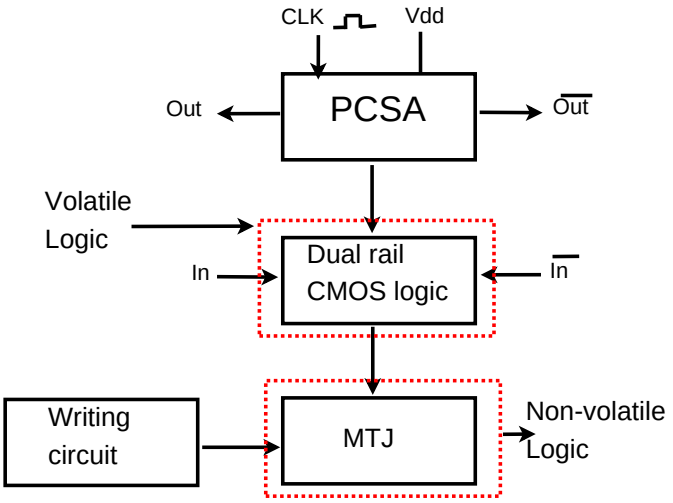



Figure 5.2: Structure of LiM based MTJ/CMOS circuits.

the outputs while the dual rail CMOS logic tree is used to evaluate the inputs. The MTJs are used to store the non-volatile data.

### 5.2.1 Operation of MTJ/CMOS circuits

The circuit operation of the MTJ/CMOS circuit is illustrated with an example of XOR based MTJ/CMOS circuit. Figure 5.3 shows the schematic of the MTJ/CMOS based XOR gate. When the clock signal is set to ground (i.e., CLK=0), the PCSA circuit pre-charges the output nodes XOR and XNOR to 1 (i.e., the output nodes are charged to Vdd). Once the clock signal CLK is set to $V_{dd}$ (i.e., CLK=1), the output voltages start discharging to ground. However, due to the difference in resistances between the orientations of the MTJ1 and MTJ2 i.e., parallel versus anti-parallel, the discharge speed will be different for each branch. So, depending on the logic inputs, one of the output node will be at $V_{dd}$ while the other node will be discharged to GND.

Let's assume MTJ1 and MTJ2 are in parallel and anti-parallel configuration respectively. Similarly, let's assume A= logic "0" and $\overline{A}$= logic "1". Since the MTJl is configured in parallel configuration and MTJ2 is configured in anti-parallel configuration, $R_{MTJl} < R_{MTJ2}$. Due to the difference in resistances between $R_{MTJl}$ and $R_{MTJ2}$, the

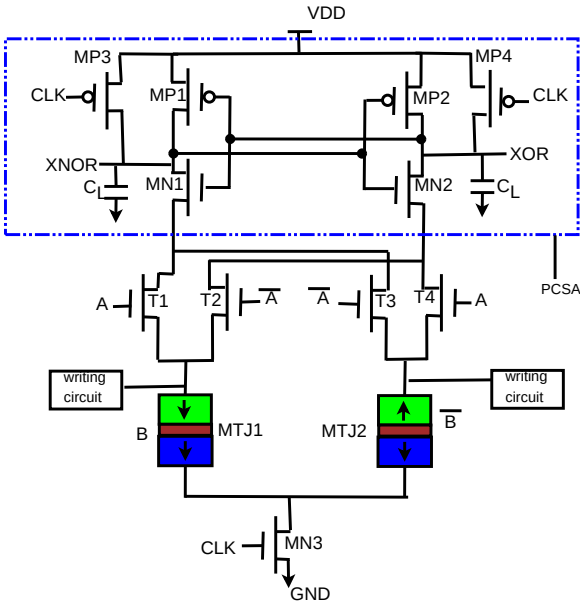



Figure 5.3: MTJ/CMOS based XOR gate [26] [22].

discharge current through MTJ1 will be greater than the discharge current through MTJ2. Thus, when XOR becomes less than the threshold switching voltage of the inverter comprised of MP1 and MN1, XNOR will be charged to 1 (i.e., $V_{dd}$) and XOR will be discharged to 0 (i.e., ground). In other words, when CLK=0, transistors MP3 and MP4 are turned ON and the outputs XOR and XNOR are pre-charged to Vdd. When CLK=1, MP3 and MP4 are turned OFF. Thus, depending on the input to the dual rail CMOS logic tree and the MTJs, one of the discharging paths will have lower resistance than the other.

### 5.2.2 Current consumption of MTJ/CMOS circuit

Figure 5.4 shows the current consumption of the MTJ/CMOS based XOR gate. The data stored in the MTJs are flipped at time T=80ns. From the Figure 5.4, we can see that the MTJ/CMOS based XOR gate has uniform current flowing into the circuit irrespective of input A if the data stored in the MTJs are constant. Uniform current consumption of the MTJ/CMOS circuit is due to the current mode logic property. In this research, we are utilizing the CML and non-volatility property of the MTJ/CMOS circuit to build a DPA

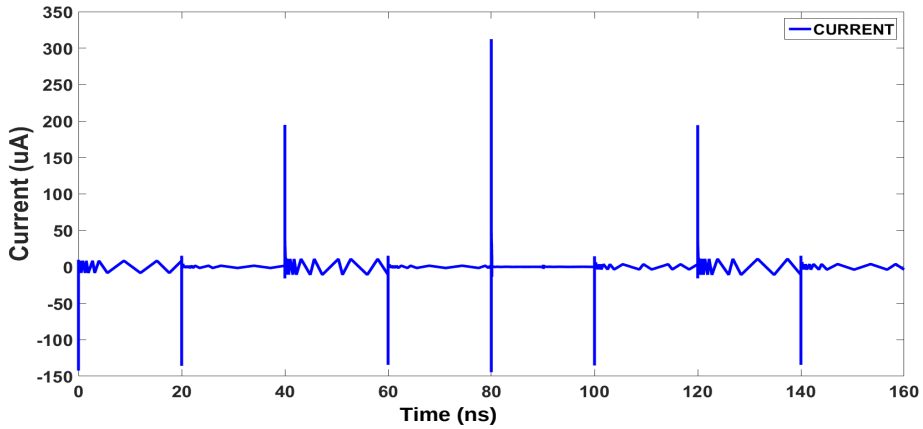



Figure 5.4: Current consumption of the MTJ/CMOS based XOR gate where the data stored in the MTJ is flipped at T=80ns.

resistant cryptographic hardware. So, we have implemented a lightweight cryptographic algorithm called PRESENT-80 using the MTJ/CMOS based circuit using Look-Up Table (LUT) method.

## 5.3 Implementation of PRESENT-80 using MTJ/CMOS logic

This section discusses the implementation of one round of PRESENT-80 cryptographic hardware using MTJ/CMOS logic circuits. In the PRESENT-80 algorithm, S-box is one of the key components for the encryption/decryption operation. S-box is the hardware block which performs the non-linear operation in the PRESENT-80 cryptographic algorithm. However, S-box is prone to Differential Power Analysis (DPA) attack due to its high power consumption. In order to reduce the power consumption and to improve its security against DPA attacks, we implemented the PRESENT-80 S-box circuit in MTJ/CMOS circuits using Look-UP Table (LUT) method.

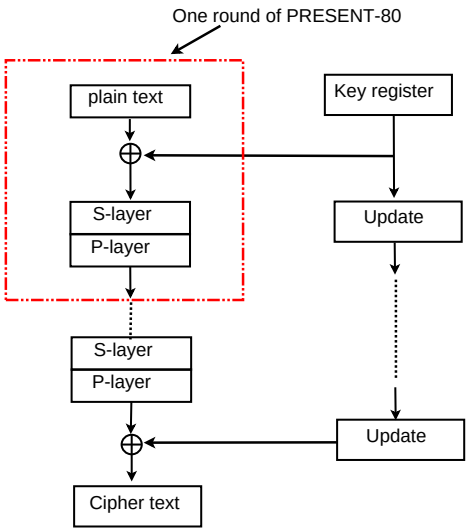



Figure 5.5: Algorithmic level description of PRESENT-80 [64].

### 5.3.1 PRESENT-80

PRESENT-80 is a light weight cryptographic algorithm with 64 bit block size and 80 or 128 bit keys [13]. For many of the low power IoT devices and RFID tags, 80 bit key based PRESENT algorithm are used for cryptographic applications (PRESENT-80). PRESENT-80 has 32 regular rounds where each round consists of key mixing step, a substitution layer (S-layer) and a permutation layer (P-layer). A top level algorithmic description of PRESENT-80 is shown Figure 5.5.

C. Rolfes et. al [64] have proposed three different architectures to implement PRESENT-80 algorithm. The different architectures are (i) Round-based architecture, (ii) Parallel architecture and (iii) a serialized architecture. Among the three architectures, round-based architecture is optimized in terms of area, speed and energy which makes it suitable to implement in low-cost IoT and RFID devices. This architecture uses only one substitution layer and permutation. So, in this dissertation, we have implemented one round of PRESENT-80 algorithm which consists of an XOR operation, S-layer and a P-layer.

- *Add round Key:* In add round key, the 64-bit round key is XORed with the 64-bit round ciper text.

Table 5.1: PRESENT S-box.

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| s[x] | C | 5 | 6 | B | 9 | 0 | A | D | 3 | E | F | 8 | 4 | 7 | 1 | 2 |

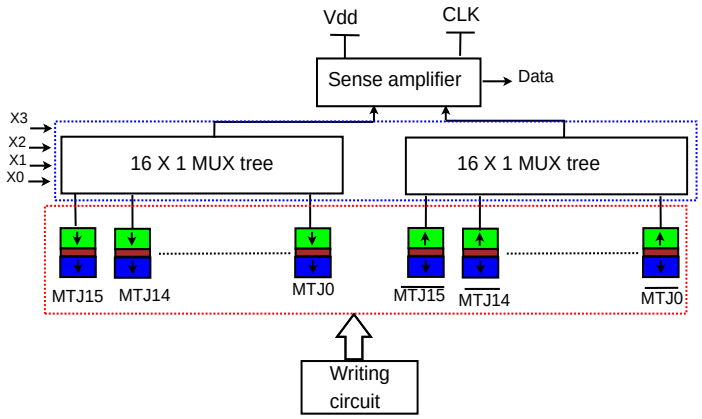



Figure 5.6: General structure of MTJ/CMOS based LUT with 4 selection lines.

- *S-layer:* Substitution layer consists of 16 S-boxes in parallel that each S-box has 4-bit input and 4-bit output. Table 5.1 shows the input and output of the PRESENT-80 S-box with hexadecimal notation.

- *P-layer:* In permutation layer (p-layer), a linear permutation is performed after the non-linear operation from the S-box. In permutation layer, there is no combinational logic.

### 5.3.2 MTJ/CMOS based Look Up Table (LUT) circuit

This section discusses the implementation of MTJ/CMOS based Look UP Table (LUT) circuit. F. Ren et al. [62] reported that MTJ/CMOS based logic circuits do not provide better energy-efficiency compared to the CMOS based logic circuit when the data stored in MTJs toggle. In other words, MTJ/CMOS logic circuits are energy efficient when they are used in applications where MTJ data are minimum toggled or zero toggled. In this research, we are built the PRESENT S-box circuit by designing a MTJ/CMOS Look Up

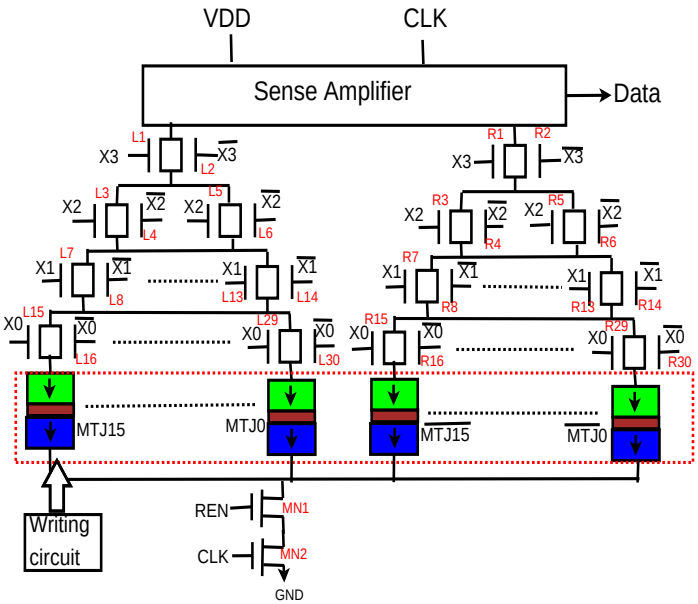



Figure 5.7: Circuit design of the MTJ/CMOS based LUT with 4 selection lines.

Table (LUT) circuit where the data stored in MTJs in S-box circuits are not toggled.

Figure 5.6 shows the general structure of the MTJ/CMOS based LUT with 4 selection lines. The MTJ data are pre-written in the MTJ by a writing circuit. In Figure 5.6, data stored in MTJ0 is read when X3=X2=X1=X0=“0”. $\overline{MTJ0}$ stores the complimentary value stored in MTJ0. For example, if logic “0” is stored in MTJ0, then logic “1” will be stored in $\overline{MTJ0}$. The data stored in the MTJ are selected by the appropriate inputs (X3, X2, X1 and X0). The data stored in the MTJ are read by the sense amplifier. One bit of the MTJ is read from each cycle of the LUT.

Figure 5.7 shows the circuit design of the MTJ/CMOS LUT with 4 selection lines. Transistors L1 to L30 and R1 and R30 are used to select the appropriate MTJ’s to read through the sense amplifier. For example, when X0=X1=X2=X3=0, transistors L2, L6, L14 and L30 are turned ON. Similarly, transistors R2, R6, R14 and R30 are turned ON. When the clk is in evaluate phase, the data stored in MTJ0 is read through a sense amplifier circuit.

Figure 5.8 shows the sense amplifier circuit to read the data stored in MTJ. The sense amplifier operates in two phases of the clock. When CLK=0, both the outputs precharge

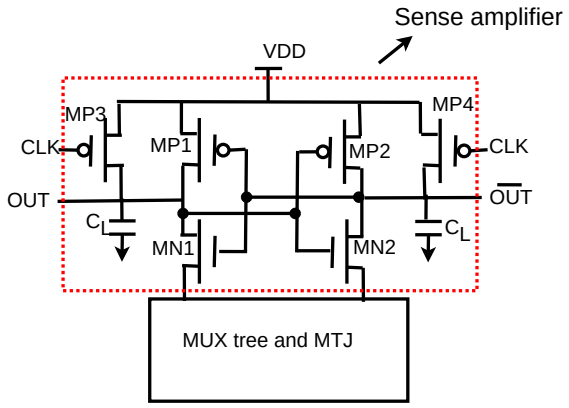



Figure 5.8: Pre-Charge Sense Amplifier (PCSA) to sense the data stored in the MTJ.

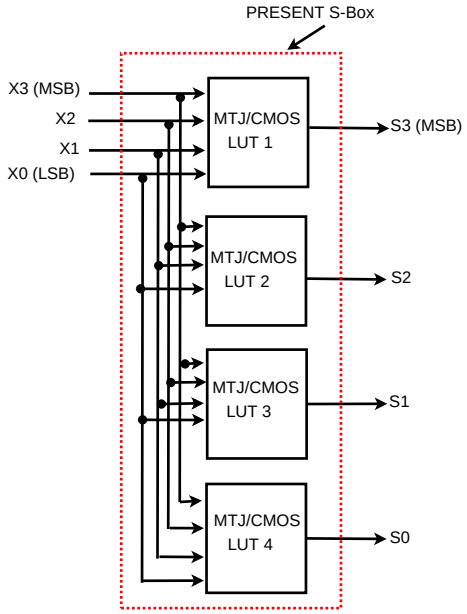



Figure 5.9: Block diagram of proposed MTJ/CMOS based PRESENT S-box

to VDD. When the CLK=1 (evaluate phase), depending on the low-resistance path, one of the output nodes will be discharged to ground while the other node will be at VDD. This property of charging the nodes to constant VDD and discharging it to ground makes the MTJ/CMOS circuit to have uniform current if the data stored in MTJ are constant.

Table 5.2: Data stored in MTJ in each LUT.

| MTJ | LUT1 | LUT2 | LUT3 | LUT4 |
|---|---|---|---|---|
| MTJ 0 | 1 | 1 | 0 | 0 |
| MTJ 1 | 0 | 1 | 0 | 1 |
| MTJ 2 | 0 | 1 | 1 | 0 |
| MTJ 3 | 1 | 0 | 1 | 1 |
| MTJ 4 | 1 | 0 | 0 | 1 |
| MTJ 5 | 0 | 0 | 0 | 0 |
| MTJ 6 | 1 | 0 | 1 | 0 |
| MTJ 7 | 1 | 1 | 0 | 1 |
| MTJ 8 | 0 | 0 | 1 | 1 |
| MTJ 9 | 1 | 1 | 1 | 0 |
| MTJ 10 | 1 | 1 | 1 | 1 |
| MTJ 11 | 1 | 0 | 0 | 0 |
| MTJ 12 | 0 | 1 | 0 | 0 |
| MTJ 13 | 0 | 1 | 1 | 1 |
| MTJ 14 | 0 | 0 | 0 | 1 |
| MTJ 15 | 0 | 0 | 1 | 0 |

### 5.3.3 MTJ/CMOS based S-box circuit

This section discusses the implementation of the MTJ/CMOS based S-box circuit. Figure 5.9 shows the block diagram of the proposed MTJ/CMOS based PRESENT S-box. The proposed idea can also be extended to any type of S-box implementation. Table 5.2 shows the data written in MTJs in each LUT. When the input X3=X2=X1=X0="0" is given as the input to the MTJ/CMOS LUT based PRESENT S-box, then S3=1, S2=1, S1=0, S1=0 is read through the sense amplifier.

Figure 5.10 shows one round of PRESENT-80 cryptographic algorithm. As discussed in the previous section, one round of PRESENT-80 can be used to implement a round based PRESENT-80 architecture. 16 S-Boxes are used in parallel to generate the 64-bit output and then outputs are permuted forming the permutation layer.

## 5.4 Energy-Efficiency Evaluation of MTJ/CMOS logic based PRESENT-80 algorithm

In this section, we compare MTJ/CMOS based one round of PRESENT-80 cryptographic algorithm with the conventional CMOS based one round of PRESENT-80 cryptographic algorithm. As discussed in Section 5.3, one round of PRESENT-80 cryptographic algorithm can be utilized to implement the whole PRESENT-80 cryptographic hardware using round based architecture. The designs are simulated using 45 nm CMOS technology with perpendicular anisotropy CoFeB/MgO MTJ model using Cadence Spectre simulator at 50MHz of operating frequency. MTJ parameters used in our simulations are given in Table 5.3 [89].

Table 5.3: MTJ device parameters used for simulations [89].

| Parameter | Description | Value |
|---|---|---|
| tsl | Thickness of the free layer | 1.3nm |
| a | Length of surface long axis | 40nm |
| b | Width of surface short axis | 40nm |
| tox | Thickness of the Oxide barrier | 0.85nm |
| TMR | Tunnel Magneto Resistance ration | 150 % |
| RA | Resistance Area Product | 5ohm$\mu m^2$ |

The conventional CMOS based one round PRESENT-80 cryptographic algorithm is implemented by using combinatorial gates in 45nm CMOS technology. The correct functionality of the MTJ/CMOS based PRESENT S-box can be verified from the transient waveforms shown in Figure 5.11.

In order to characterize the CMOS and MTJ/CMOS designs in equivalent condition, 32 D Flip-Flops are added to CMOS based one round of PRESENT-80 cryptographic hardware to synchronize the outputs with clock signal as PCSA based MTJ/CMOS circuits are naturally synchronized. Further, it has to be noted that in our MTJ/CMOS based PRESENT S-box design, data are written only one time. Once the data are written in the S-box circuit, there is no need to flip the data stored in the MTJs. The constant storage of data in

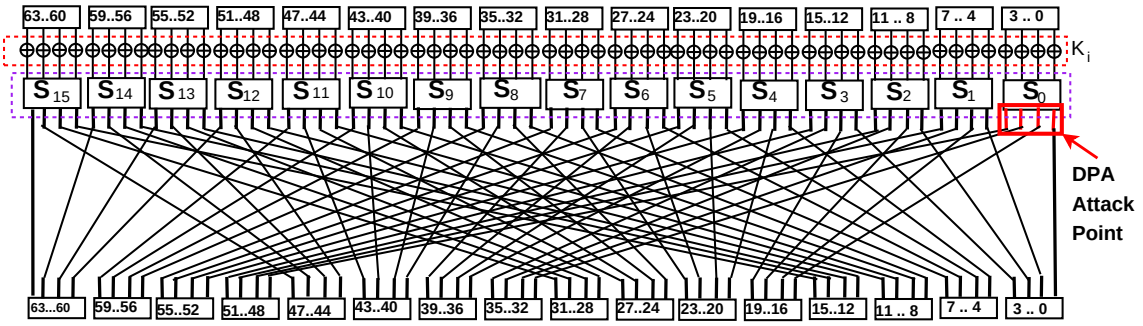



Figure 5.10: Implementation of one round of PRESENT-80.

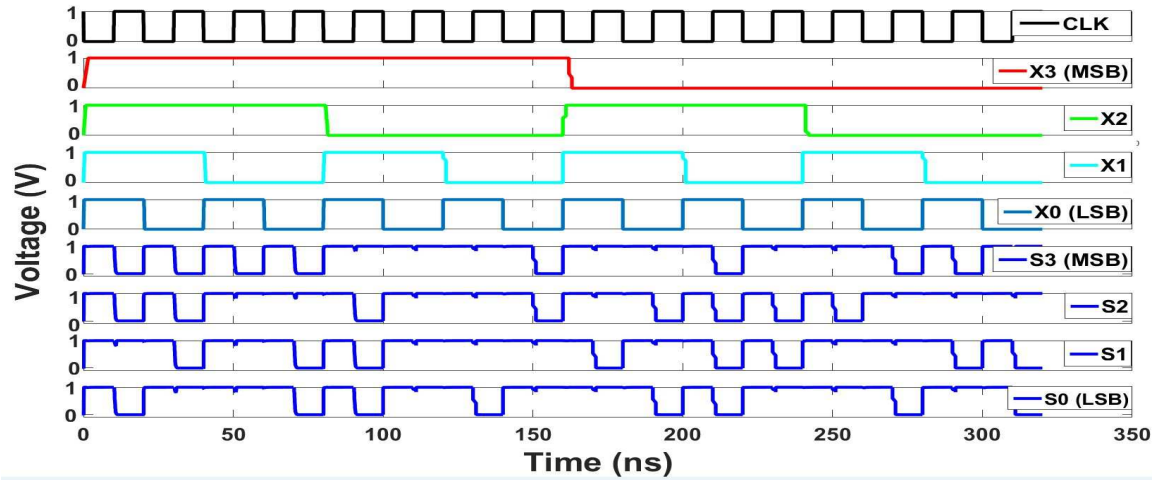



Figure 5.11: Transient waveforms of the PRESENT S-box circuit implemented using MTJ/CMOS circuits in LUT method.

MTJs without toggling helps in improving the overall energy-efficiency of the MTJ/CMOS circuits. In our designs, we have assumed that the secret key stored are permanent and there won't be any update on the secret key. However, for applications where there is a frequent update on secret key, MTJ/CMOS based XOR gate can be replaced by existing DPA resistant XOR logic families [37], [75].

Table 5.4 shows the performance comparison of the MTJ/CMOS and CMOS based implementation of the PRESENT-80 cryptographic module. We have implemented the PRESENT-80 S-box circuit and one round of PRESENT-80 cryptographic algorithm. From Table 5.4, we can see that the MTJ/CMOS based PRESENT-80 S-box circuit saves up to 26% of energy/cycle and 28% of power compared to the CMOS based implementa-

Table 5.4: Performance comparison of MTJ/CMOS and CMOS based implementation of PRESENT-80.

| Design | Energy/cycle | Avg. Power | Delay |
|---|---|---|---|
| 4x4 PRESENT S-box (MTJ/CMOS) | 24.3 fJ | 1.23 $\mu$W | 402.5 ps |
| 4x4 PRESENT S-box (CMOS) | 32.4 fJ | 1.72 $\mu$W | 312.8 ps |
| PRESENT-80 (MTJ/CMOS) | 402.96 fJ | 20.65 $\mu$W | 640.8 ps |
| PRESENT-80 (CMOS) | 566.8 fJ | 28.336 $\mu$W | 484.3 ps |

tion. Similarly, one round of PRESENT-80 cryptographic algorithm implemented using MTJ/CMOS circuit saves up to 29% of energy/cycle and 27% of power compared to the CMOS based implementation. Though the delay of the MTJ/CMOS circuits are more than the conventional CMOS based circuits, the overall Power Delay Product (PDP) of MTJ/CMOS and CMOS based cryptographic module are comparable. For example, PDP of one round of MTJ/CMOS based PRESENT-80 is 4% lower than the CMOS based implementation of PRESENT-80. Further, usage of MTJ in MTJ/CMOS circuits has several advantages such as high density, non-volatility and lower leakage compared to the CMOS based implementation.

## 5.5 Security Evaluation of MTJ/CMOS logic based PRESENT S-box

This section discusses the security evaluation of the MTJ/CMOS circuits. Security evaluation is performed by performing a DPA attack on the PRESENT S-box built using the MTJ/CMOS circuits and CMOS circuits using the steps described in Chapter 2. In this dissertation, we simulated the S-box circuit at 50 MHz where the period of each clock corresponds to $20ns$. We have sampled the current traces with a time period of $4ps$. So, each input plain text corresponds to 5000 measured points.

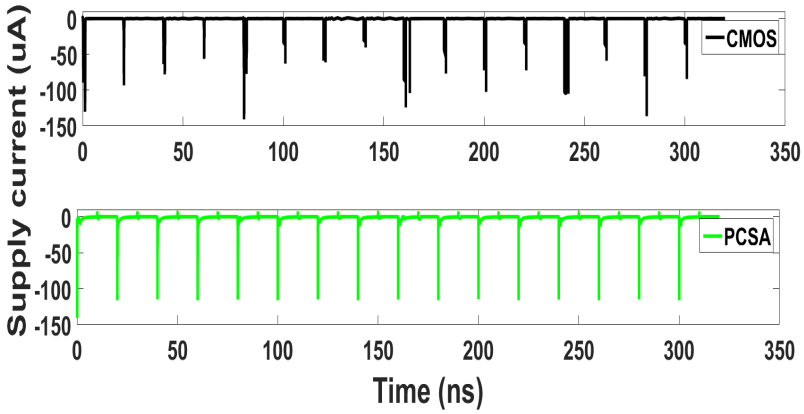



Figure 5.12: Current consumption of the CMOS and MTJ/CMOS implementation of PRESENT S-box.

### 5.5.1 Test case for MTJ/CMOS based S-box circuit

In our test case, the key was chosen to be $(6)_{10}$. A correlation co-efficient based DPA attack was performed on PRESENT-80 S-box circuit implemented using MTJ/CMOS circuit and conventional CMOS based PRESENT-80 S-box circuit. Test circuit consists of four XOR gates performing Add Round Key operation and the PRESENT-80 based S-box circuit together. In the real life DPA attacks, a large number (greater than 100,000 plain texts) of input plain texts are fed to the cryptographic processor. However, we are performing the simulation based DPA attack without any electrical noises. Moreover, test chip was not a full chip with other analog and digital modules of the crypto processor that consume additional current. So, for our CMOS based S-box circuit, the secret key was revealed using only 14 power traces. We have to note, that the electrical noises present in the chip increases the number of traces required to break the crypto processor. For our test case simulations, we consider the ideal environment (without noise) for an attacker to perform DPA attack. The same environment has been used to perform DPA attack in MTJ/CMOS circuits. Figure 5.12 shows the uniform current flowing in the MTJ/CMOS based PRESENT-80 S-box circuit while non-uniform current flowing in the CMOS based PRESENT-80 S-box circuit.

Figure 5.13 shows the successful DPA attack on PRESENT-80 S-box circuit implemented using the CMOS based S-box circuit. It has to be noted that the successful DPA

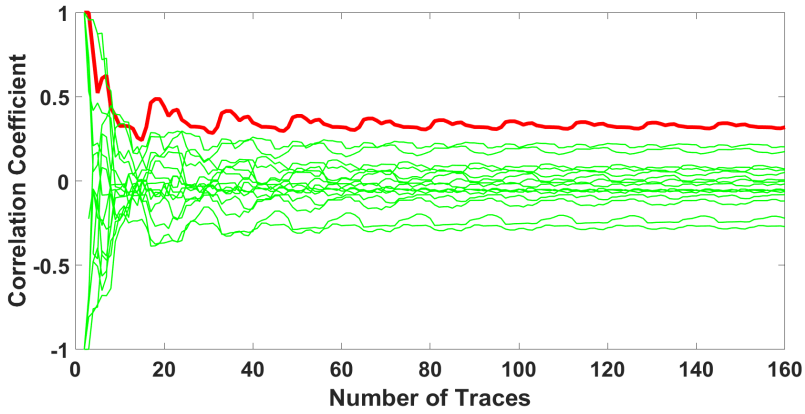



Figure 5.13: A successful DPA attack on PRESENT S-box implemented using conventional CMOS logic gates with key=06.

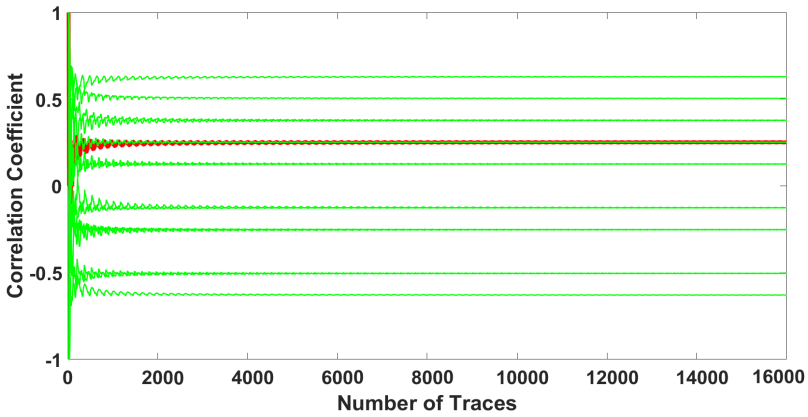



Figure 5.14: An unsuccessful DPA attack on PRESENT S-box implemented using MTJ/CMOS circuit with key=06.

attack on CMOS based PRESENT S-box circuit is due to the correlation between the input data and the power traces. Figure 5.14 shows the unsuccessful DPA attack after 16,000 power traces. The unsuccessful DPA attack on MTJ/CMOS based PRESENT S-box circuit is due to the uniform power consumption of the MTJ/CMOS circuit irrespective of the input data transitions. It has to be noted that in our simulations, XOR gate in the MTJ/CMOS implementation of PRESENT-80 is implemented using the MTJ/CMOS XOR gate where the key is stored in the MTJ devices.

## 5.6 Summary

In this chapter, we have explored the usefulness of designing MTJ/CMOS based cryptographic circuits and evaluated its resilience against the DPA attack. MTJ/CMOS circuits consume uniform power if there is no switching of MTJ devices. We have investigated the novel approach of building cryptographic hardware in MTJ/CMOS circuits using Look-Up Table (LUT) based approach where the data stored in MTJs are constant during the entire encryption/decryption operation. As a case study, we have implemented a S-box circuit and one round of the PRESENT-80 lightweight cryptographic algorithm using Look-Up Table (LUT) method. From our simulations, we found that the MTJ/CMOS based PRESENT-80 is resistant against DPA attack. Further, PRESENT-80 S-box circuit and one round of PRESENT-80 implemented using MTJ/CMOS circuit saves up to 26% of power and 29% of energy compared to the CMOS based implementation, respectively. The Low-energy and DPA resistant property along with high density and low-leakage make hybrid MTJ/CMOS circuits to become a suitable candidate for building non-volatile, low-energy and compact embedded cryptographic hardware modules which can be resistant against DPA attack.

# Chapter 6

# Energy-Efficient Design of MTJ/CMOS Logic for DPA Secure Hardware

Hybrid MTJ/CMOS-based Logic-in-Memory (LiM) architecture-based circuits show high potential in designing low-power circuits by reducing the leakage power. Currently, high supply voltage ($V_{dd}$) is required in both writing and sensing operations of LiM circuits, which consumes considerable amount of energy. In order to meet the power budget in low-power electronic devices, scaling down of $V_{dd}$ is used as an effective method to reduce the dynamic power consumption. However, scaling down of Vdd leads to increase in leakage power. Furthermore, the effectiveness of $V_{dd}$ scaling has declined at a point where further reduction in $V_{dd}$ leads to incorrect circuit operation or decrease in energy efficiency of the circuits. In this chapter, we propose a novel energy-efficient and Secure MTJ/CMOS Logic (SMCL) circuits to design ultra-low-power MTJ/CMOS circuits. Similar to the existing MTJ/CMOS designs, the proposed MTJ/CMOS design also works in two different modes of clock. The proposed MTJ/CMOS designs have considerable power savings during the pre-charge of the clock. During the pre-charge phase, both output nodes are pre-charged to $V_{dd}/2$, while during the evaluate phase, one node will be charged to VDD, while the other node will discharged to ground. Moreover, the proposed SMCL consumes uniform power

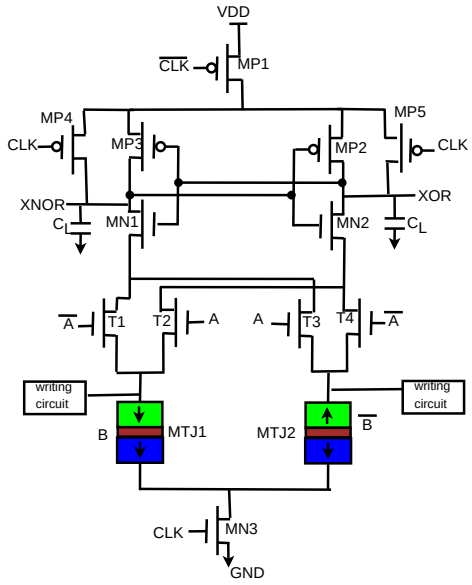



Figure 6.1: Schematic of the proposed SMCL based XOR gate.

by masking the MTJ during the write operation from the power supply thereby thwarting the power analysis based side-channel attacks.

## 6.1 Proposed Secure MTJ/CMOS Logic (SMCL) circuits

This section explains the operation of the proposed Secure MTJ/CMOS Logic (SMCL) circuits. In the proposed SMCL circuit, the MTJ's are masked from the power supply during the data are written to the MTJ. If the MTJ value is not changed, then both PCSA and SMCL circuits will consume uniform power. However, our proposed SMCL based MTJ/CMOS logic gates are more energy-efficient than the existing PCSA based MTJ/CMOS logic gates.

### 6.1.1 Operation of the proposed SMCL circuit

This section explains the operation of the proposed SMCL circuit. The circuit operation of the proposed SMCL circuit is explained by the operation of an XOR gate. Figure 6.1 shows the schematic diagram of the proposed SMCL based XOR gate. Transistor MP1 is used to disconnect the MTJ from $V_{dd}$ when the data is written in it. Transistors MP2, MP3,

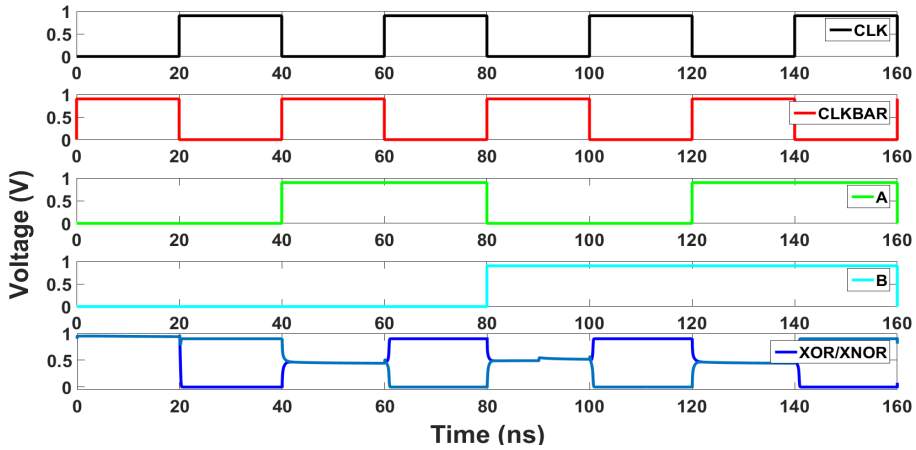



Figure 6.2: Transient analysis of the proposed SMCL based XOR gate.

MN1 and MN2 are used to stabilize the outputs. Transistors MP4 and MP5 are used for charge sharing between the output nodes.

The operation of the proposed SMCL circuit is explained with the example of XOR gate through each phase of the clock.

**Charge-sharing phase:** During the charge-sharing phase, CLK=0, $\overline{CLK}$=1. When CLK=0, transistor MP4 and MP5 will be turned ON. Since, the proposed SMCL XOR gate is dual rail in nature, the outputs will be shared between the output nodes during the charge-sharing phase. During the charge-sharing phase, MP1 is turned OFF to mask the MTJ while writing the data in the MTJ's. Moreover, in the proposed SMCL circuits, the outputs are precharged to $V_{dd}/2$ unlike the conventional PCSA MTJ/CMOS circuit where the outputs are precharged to $V_{dd}$. Since, the outputs are precharged to $V_{dd}/2$, the proposed SMCL circuits consume low power compared to the existing PCSA based MTJ/CMOS circuits.

**Evaluate phase:** During the evaluate phase, CLK=1, $\overline{CLK}$=0. In this phase, transistor MP1 and MN3 will be turned ON and MP4 and MP5 will be turned OFF. For analysis, let us assume that the input A=0, B=1. When A=0, transistor T2 and T3 will be turned OFF while T1 and T4 will be turned ON. The resistance of MTJ1 will be less as compared to resistance of MTJ2. When CLK=1, the charge stored in XNOR output will be discharged to ground

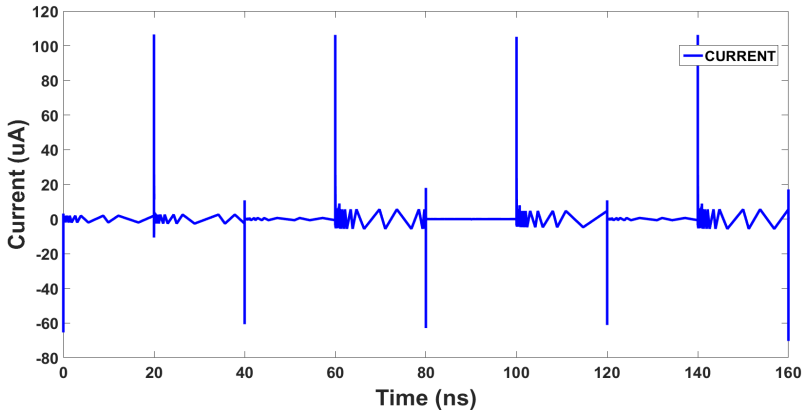



Figure 6.3: Current consumption of the proposed SMCL based XOR gate.

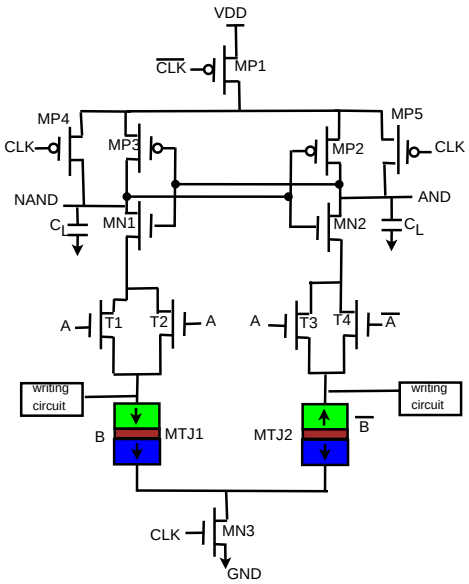



Figure 6.4: Schematic of the proposed SMCL AND gate.

through T1 and MTJ2 which makes transistor MN2 to turn OFF. Since, the transistor MN2 is turned OFF, the XOR output will be charged to $V_{dd}$. The transient waveforms of the proposed SMCL XOR gate is shown in Figure 6.2. Figure 6.3 shows the uniform current consumption of the proposed SMCL XOR gate. Figure 6.4 shows the schematic of the proposed SMCL AND gate.

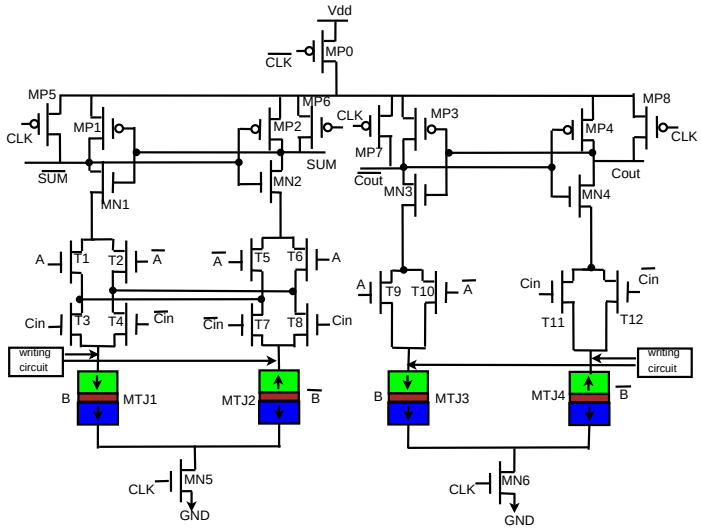



Figure 6.5: Schematic of the proposed SMCL based full adder circuit

### 6.1.2 Proposed MTJ/CMOS full adder circuit

Figure 6.5 shows the schematic of the proposed SMCL based Magnetic Full Adder (MFA). The inputs for the full adder are “A”, “B” and “Cin” and the outputs are SUM and Cout. In the proposed magnetic full adder circuit, MP1 to MP8 and MN1 to MN4 are used as the sense amplifier. MP0 is used to mask the MTJ during the write operation. Rest of the transistors are used for evaluating SUM and Cout outputs. The MOS tree structure of the ERLIM based magnetic full adder is based on the following equations:

$$Sum = A.B.Cin + \overline{B}.A.\overline{Cin} + \overline{A}.B.\overline{Cin} + \overline{A}.Cin.\overline{B} \tag{6.1}$$

$$Cout = A.B + A.Cin + B.Cin \tag{6.2}$$

Let us assume that B=“1” and $\overline{B}$=“0” and A=1 and Cin=1. At T1 phase of the CLK, all the inputs are passed to the circuit and the non-volatile data is stored in the MTJs. At T2 phase of the CLK, the inputs are evaluated by the CMOS logic tree. For A=1 and Cin=1, $\overline{Sum}$ will be discharged faster through the transistors T1 and T3. and SUM output will be charged to $V_{dd}$. Similarly, $\overline{Cout}$ will be discharged to ground through T9 transistor and

Cout will be charged to Vdd. At T3 phase of the CLK, the outputs will be hold. At T4, CLK slowly decrease from Vdd to gnd. So, the charge stored at the SUM and Cout will be recovered back to CLK.

### 6.1.3 Theoretical analysis of energy consumption in the proposed SMCL circuit

This section theoretically analyze the energy consumption in the proposed SMCL circuit with the existing PCSA based MTJ/CMOS circuit. For analysis lets consider the PCSA based MTJ/CMOS XOR gate and the proposed SMCL based XOR gate (Figure 6.1).

**Energy consumption in PCSA based MTJ/CMOS XOR gate**

The energy dissipated to charge a capacitor is given by,

$$E_{diss} = \frac{1}{2}CV_{dd}^2 \tag{6.3}$$

where, C is the capacitance value and $V_{dd}$ is the voltage swing.

During the pre-charge phase of the CLK, both XOR and XNOR outputs are charged to $V_{dd}$. Assuming that one of the ouput will be charged to $V_{dd}$ in the previous cycle, the total energy dissipated to charge the load capacitors is given by.

$$E_{diss,pre-charge} = \frac{1}{2}CV_{dd}^2 \tag{6.4}$$

Similarly during the evaluate phase of the CLK, one of the two outputs (XOR or XNOR) will be discharged to ground while the other output will be at $V_{dd}$. So, the energy dissipated during the evaluate phase of the CLK is given by,

$$E_{diss,eval} = \frac{1}{2}CV_{dd}^2 \tag{6.5}$$

So, the total energy dissipated in one clock cycle of the PCSA based MTJ/CMOS XOR gate is given by,

$$E_{diss,PCSA} = E_{diss,pre-charge} + E_{diss,eval} \tag{6.6}$$

$$E_{diss,PCSA} = CV_{dd}^2 \tag{6.7}$$

The total energy dissipated in one clock cycle of the PCSA based MTJ/CMOS XOR gate is given as $CV_{dd}^2$.

**Energy consumption in proposed SMCL XOR gate**

Let us assume that one of the outputs are already charged to $V_{dd}$ during the previous cycle. During the charge sharing phase of the proposed SMCL XOR gate (Figure 6.1), output voltages will be pre-charge to $V_{dd}$/2. During this phase, the charge and voltage are divided equally between the two load capacitors (XOR and XNOR). So, the total energy dissipated in the charge sharing phase of the proposed SMCL XOR gate is given by,

$$E_{diss,charge-sharing} = \frac{1}{4}CV_{dd}^2 \tag{6.8}$$

Similarly during the evaluate phase of the CLK, one of the two outputs (XOR or XNOR) will be discharged to ground while the other output will be charged to $V_{dd}$. So, the energy dissipated during the evaluate phase of the CLK is given by,

$$E_{diss,eval} = \frac{1}{2}C(V_{dd}/2)^2 + \frac{1}{2}C(V_{dd}/2)^2 \tag{6.9}$$

$$E_{diss,eval} = \frac{1}{4}CV_{dd}^2 \tag{6.10}$$

So, the total energy dissipated in one clock cycle of the proposed SMCL XOR gate is

given by,

$$E_{diss,proposed} = E_{diss,charge-sharing} + E_{diss,eval} \tag{6.11}$$

$$E_{diss,proposed} = \frac{1}{2}CV_{dd}^2 \tag{6.12}$$

The total energy dissipated in one clock cycle of the proposed SMCL XOR gate is given as $0.5CV_{dd}^2$ which is 50% less than the existing PCSA based MTJ/CMOS XOR gate.

Table 6.1: Performance comparison of PCSA based XOR gate and proposed SMCL XOR gate.

| | **PCSA based XOR [22]** | **Proposed SMCL XOR gate** | **% impr.** |
|---|---|---|---|
| **Avg. energy (fJ)** | 3.604 | 1.871 | 50 |
| **Avg. power (nW)** | 40.34 | 23.1 | 42.7 |
| **Device count** | 11MOS +2MTJ | 12MOS+2MTJ | - |

Table 6.2: Performance comparison of PCSA based AND gate and proposed SMCL AND gate.

| | **PCSA based AND [22]** | **Proposed SMCL AND gate** | **% impr.** |
|---|---|---|---|
| **Avg. energy (fJ)** | 3.414 | 1.768 | 50 |
| **Avg. power (nW)** | 38.24 | 21.37 | 44.11 |
| **Device count** | 10MOS +2MTJ | 12MOS+2MTJ | - |

Table 6.3: Performance comparison of PCSA based full adder and proposed full adder circuit.

| | **PCSA based full adder [22]** | **Proposed SMCL full adder** | **% impr.** |
|---|---|---|---|
| **Avg. energy (fJ)** | 115.4 | 60.84 | 47.27 |
| **Avg. power (nW)** | 360.5 | 208.9 | 42.05 |
| **Device count** | 25MOS +4MTJ | 26MOS+2MTJ | - |

Table 6.4: Simulated and calculated results for XOR gate for various DPA-resistant adiabatic logic families.

| Logic family | PCSA based XOR gate | Proposed XOR gate |
|---|---|---|
| $E_{min}$(fJ) | 2.9 | 1.431 |
| $E_{max}$(fJ) | 6.3 | 1.85 |
| NED (%) | 69.3 | 2.63 |
| NSD(%) | 61.27 | 1.23 |

Table 6.5: Simulated and calculated results for AND gate for various DPA-resistant adiabatic logic families.

| Logic family | PCSA based AND gate | Proposed SMCL AND gate |
|---|---|---|
| $E_{min}$(fJ) | 2.77 | 1.25 |
| $E_{max}$(fJ) | 6.56 | 2.9 |
| NED (%) | 75.2 | 5.4 |
| NSD(%) | 64.33 | 3.22 |

## 6.2 Simulation results of SMCL based Logic Gates

This section presents the simulation results of the proposed SMCL circuits. Simulations are performed using Cadence Spectre simulator with 45nm standard CMOS technology with perpendicular anisotropy CoFeB/MgO MTJ model. The MTJ device parameters used for simulations in this work are shown in Table 5.3 [83]. The simulations are performed at 50 MHz with $V_{dd}$=0.9V and load capacitor is 1fF.

The size of all the transistors are W/L=120nm/45nm. Table 6.1 gives the comparison of the PCSA based XOR gate and the proposed SMCL XOR gate. From Table 6.1, we can see that the proposed SMCL XOR gate has 50% energy savings compared to the existing PCSA based XOR gate which is same as the results obtained in theoretical analysis in Section 6.1.3.

Table 6.2 shows the comparison of the PCSA based AND gate and the proposed AND gate. From Table 6.2, we can see that the proposed SMCL AND gate has 42.7% and 50% of power and energy savings compared to the existing PCSA based AND gate. From Table 6.3, we can see that the proposed SMCL based FA consumes 47.27% less energy

consumption as compared to the existing PCSA based FA.

### 6.2.1 Security metrics analysis of the MTJ/CMOS gates

This section discusses the security metric analysis of the MTJ/CMOS gates. The parameter Normalized Energy Deviation (NED), defined as $(E_{max} - E_{min})/E_{max}$, is used to indicate the percentage difference between minimum and maximum energy consumption for all possible input transitions. Normalized Standard Deviation (NSD) indicates the energy consumption variation based on the inputs and it is calculated as $\frac{\sigma_E}{\bar{E}}$. $\bar{\text{E}}$ denotes the average energy dissipation for various input transitions. In general, '$n$' input gate will have $2^{2n}$ possible input transitions. For example, 2 input gates will have 16 input transitions. $\sigma_E$ denotes the standard deviation of the energy dissipated by the circuit and it is given by $\sigma = \sqrt{\frac{\sum_{i=1}^{n}(E_i - \bar{E})^2}{n}}$.

From Table 6.4 and Table 6.5, we can see that the NED and NSD values for the proposed SMCL circuit is very less than the existing PCSA based MTJ/CMOS circuit. Lower the values of NED and NSD, higher the resilience of the circuit towards power analysis attack.

## 6.3 Analysis of SMCL based PRESENT-80 cryptographic hardware

This section discusses the energy-efficiency and security analysis of the proposed SMCL based PRESENT-80 cryptographic hardware. MTJ/CMOS logic circuits are not energy-efficient compared to the CMOS based logic circuit when data stored in MTJs toggle [62]. As proposed in Chapter 5, we have used the Look Up Table (LUT) method to implement PRESENT-80 cryptographic hardware in proposed SMCL logic.

Figure 6.6 shows the sense amplifier circuit to read the data stored in MTJ. Figure 6.6 (a) shows the existing PCSA based sense amplifier and Figure 6.6 (b) shows the proposed SMCL based sense amplifier circuit. As discussed in previous section, SMCL based circuit

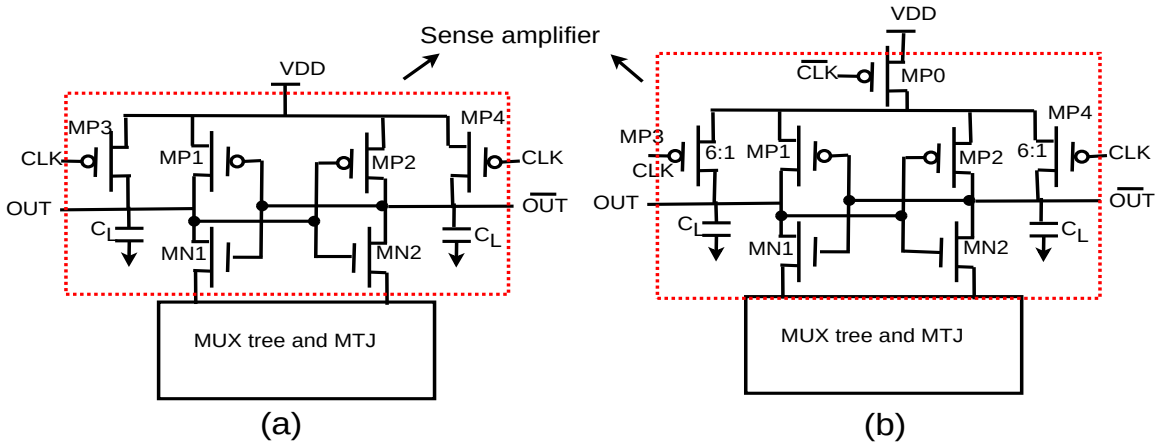



Figure 6.6: a) PCSA based sense amplifier, b) Proposed SMCL based sense amplifier circuit.

are more energy-efficient than the PCSA based circuit due to pre-charging the output nodes to $V_{dd}/2$. So, in order to have charge sharing, we increase the width MP3 and MP4 to 6 times than the other PMOS transistors (refer Figure 6.6 (b)). As we know, increasing the width of transistors reduces the resistance which helps to charge share the output nodes fast.

Figure 6.7 shows the transient waveforms of the PRESENT-S-box circuit implemented using the proposed SMCL logic based sense amplifier circuit. The MTJs in the SMCL based PRESENT-80 S-box circuit are used to store the S-box data while the CMOS logic is used to choose the corresponding data from the MTJ. SMCL based sense amplifier is used to read the data stored in the MTJs. As discussed in previous section, SMCL based circuits pre-charge the output nodes to $V_{dd}/2$ which improves its energy-efficiency compared to existing PCSA based circuits. In Figure 6.7, X0, X1, X2, and X3 represent the input to the S-box while S0, S1, S2, and S3 represent the corresponding output of the SMCL based PRESENT-80 S-box circuit.

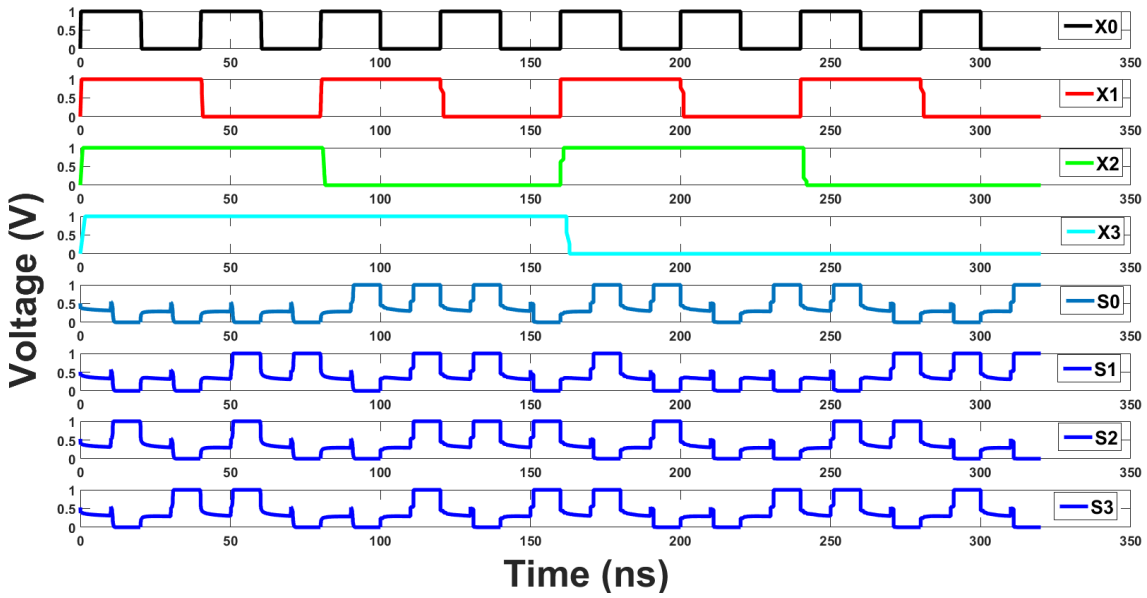



Figure 6.7: Transient waveforms of the PRESENT S-Box circuit implemented using proposed SMCL logic based sense amplifier.

### 6.3.1 Energy-Efficiency analysis of SMCL based PRESENT-80 cryptographic hardware

This section presents the energy-efficiency analysis of the SMCL based PRESENT-80 cryptographic hardware. We initially implemented a PRESENT-80 S-box circuit using the existing state-of-art PCSA based MTJ/CMOS circuit (refer chapter 5) and proposed SMCL based circuits. Further, we have also implemented CMOS based PRESENT-80 S-box circuit to compare its energy-efficiency with the proposed SMCL based PRESENT-80 S-box circuit. In order to characterize the CMOS and MTJ/CMOS designs in equivalent condition, 32 D Flip-Flops are added to CMOS based one round of PRESENT-80 cryptographic hardware to synchronize the outputs with clock signal as PCSA based MTJ/CMOS circuits are naturally synchronized. Further, it has to be noted that in our MTJ/CMOS based PRESENT S-box design, data are written only one time. Once the data are written in the S-box circuit, there is no need to flip the data stored in the MTJs. The constant storage of data in MTJs without toggling helps in improving the overall energy-efficiency of the MTJ/CMOS circuits.

Table 6.6: Energy consumption comparison of PRESENT-80 S-box circuit.

| Implementation | Energy/cycle | Avg. Power | Energy savings |
|---|---|---|---|
| PCSA based MTJ/CMOS | 24.3 fJ | 1.23 $\mu$W | 45% |
| CMOS | 32.4 fJ | 1.72 $\mu$W | 59% |
| Proposed SMCL based MTJ/CMOS | 13.4 fJ | 0.74 $\mu$W | - |

Table 6.6 shows the energy consumption comparison of the PRESENT-80 S-box circuit implemented using PCSA based MTJ/CMOS, conventional CMOS circuit and proposed SMCL based MTJ/CMOS circuit. From the table, we can see that the proposed SMCL based MTJ/CMOS implementation of PRESENT-80 S-box circuit saves up to 59% of energy as compared to the conventional CMOS based PRESENT-80 S-box circuit. Moreover, the proposed SMCL based MTJ/CMOS based PRESENT-80 S-box circuit saves up to 45% of energy/cycle.

Table 6.7: Energy consumption comparison of PRESENT-80 cryptographic hardware.

| Implementation | Energy/cycle | Avg. Power | Energy savings |
|---|---|---|---|
| PCSA based MTJ/CMOS | 402.96 fJ | 20.65 $\mu$W | 42.18% |
| Conventional CMOS | 566.8 fJ | 28.336 $\mu$W | 59% |
| Proposed SMCL based MTJ/CMOS | 232.96 fJ | 12.65 $\mu$W | - |

Further, in this research, we have also implemented one round of PRESENT-80 cryptographic hardware with the proposed SMCL based MTJ/CMOS circuit. Table 6.7 shows the energy consumption comparison of the PRESENT-80 cryptographic hardware implemented using PCSA based MTJ/CMOS, conventional CMOS based circuits and proposed SMCL based MTJ/CMOS. From our simulations, we can see that the proposed SMCL based MTJ/CMOS saves up to 42.18% of energy as compared to the PCSA based MTJ/CMOS circuits. Further, SMCL based MTJ/CMOS PRESENT-80 cryptographic hardware saves up to 59% of energy as compared to the conventional CMOS based PRESENT-80 cryptographic hardware.

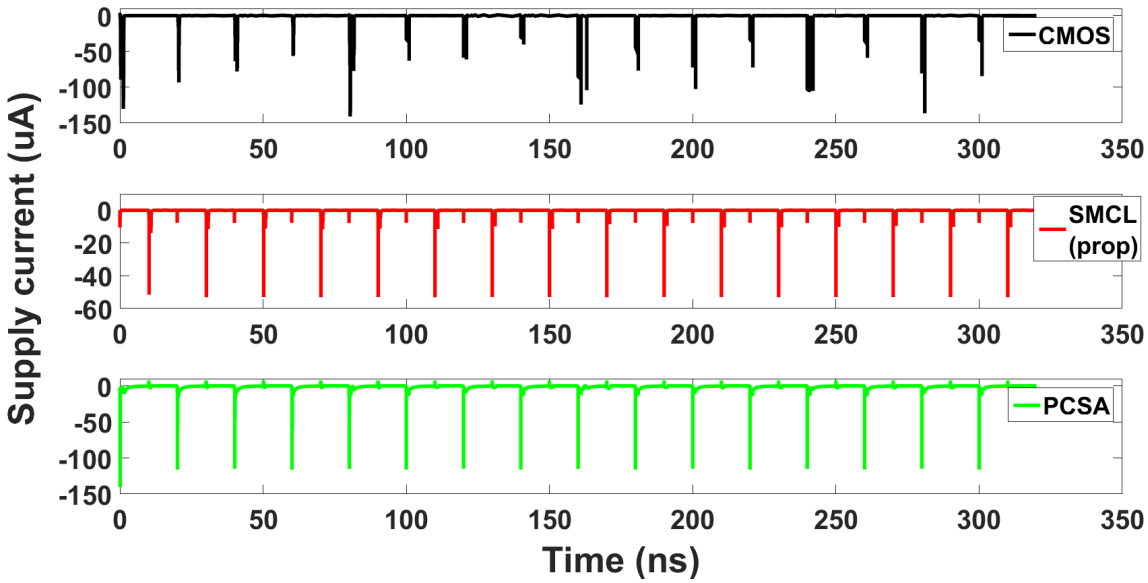



Figure 6.8: Current consumption of the CMOS, proposed SMCL based MTJ/CMOS and PCSA based MTJ/CMOS implementation of PRESENT S-Box.

### 6.3.2 Security analysis of SMCL based PRESENT-80 cryptographic hardware

This section presents the security analysis of the SMCL based PRESENT-80 cryptographic hardware. Figure 6.8 shows the current consumption of the PRESENT-80 S-box circuit implemented using conventional CMOS circuits, proposed SMCL based MTJ/CMOS circuits and PCSA based MTJ/CMOS circuits. From the Figure 6.8, we can see that the conventional CMOS based PRESENT-80 S-box circuit had non-uniform power consumption which makes it susceptible to DPA attack. In this research, we have used the look-up table based method (refer Chapter 5) to implement the cryptographic circuit using MTJ/CMOS circuit. From Figure 6.8, we can see that the proposed SMCL MTJ/CMOS based PRESENT-80 S-box circuit has reduced uniform current consumption compared to the PCSA MTJ/CMOS based PRESENT-80 S-box circuit. Figure 6.9 shows the non-successful DPA attack on the proposed SMCL based PRESENT-80 S-box circuit with key=06.

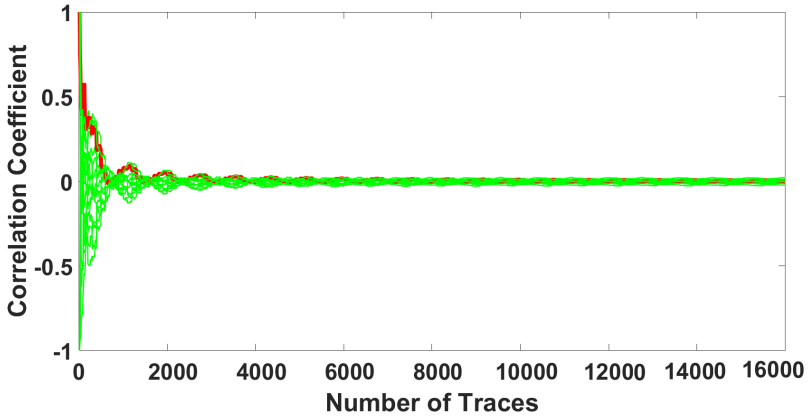



Figure 6.9: A non-successful DPA attack on PRESENT S-box implemented using proposed SMCL logic with key=06.

## 6.4 Summary

In this chapter, we have proposed energy-efficient Secure MTJ/CMOS logic family. The proposed MTJ/CMOS logic is energy-efficient compared to the existing PCSA based MTJ/CMOS by pre-charging the output nodes to $V_{dd}/2$. Further, we have implemented a PRESENT-80 lightweight cryptographic hardware using the proposed SMCL logic. From our simulations, we observed that the proposed SMCL based PRESENT-80 cryptographic hardware has about 42% and 59% of energy savings compared to the PCSA based MTJ/CMOS and conventional CMOS based implementation, respectively. Further, we have also performed the DPA attack on the SMCL based PRESENT-80 and the secret key was not revealed after 16000 power traces. The low-energy and DPA resistant property makes the proposed SMCL logic a suitable circuit design technique suitable for low-power non-volatile memory based IoT devices.

# Chapter 7

# Adiabatic Logic Based Energy Efficient and Reliable PUF for IoT devices

Apart from Differential Power Analysis (DPA) based side-channel attack on IoT devices, authentication and piracy also needs to be addressed [48]. It is expected that there will be more than 50 billion IoT devices in the real world market. Further, most of the IoT devices are deployed in places where less human operators are sitting behind. So, these devices must be capable of identifying and authenticating themselves. The second concern for the IoT devices is the cloning attack. IoT devices are deployed in open. An attacker may easily access an IoT device and extract the secret keys to clone the device. Currently, the secret keys used for authentication are stored in non-volatile memories. However, the secret keys are vulnerable to active attacks [48], [4], [40]. Moreover, implementing a tamper resistant circuitry in IoT devices to provide high level physical security may be very expensive in terms of cost and energy. Physically Unclonable Functions (PUFs) are a class of circuits that use the inherent variations in an Integrated Circuit (IC) manufacturing process to create unique and unclonable IDs. PUFs have shown great promise for generating secure key generation for the cryptographic hardware in an inexpensive way. However, designing a reliable PUF along with energy-efficiency is a big challenge. In this chapter, we propose

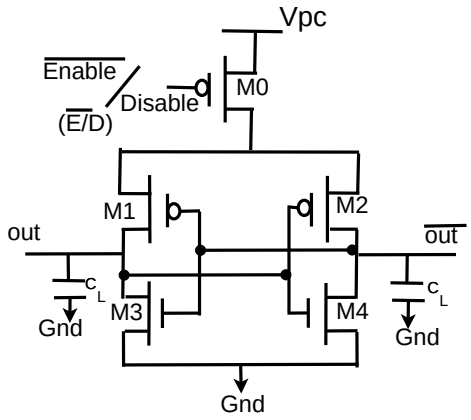



Figure 7.1: Schematic of the proposed adiabatic logic based PUF cell.

a novel energy-efficient adiabatic logic based PUF structure for energy-efficiency and reliable key generation. The proposed adiabatic PUF uses energy recovery concept to achieve high energy efficiency and uses the time ramp voltage to exhibit the reliable start-up behavior.

## 7.1 Proposed adiabatic logic based PUF

Time ramp voltages are used in adiabatic logic technique to recover the energy from each node of the circuit. In this chapter, we propose a novel adiabatic logic based PUF that utilizes the unique property of adiabatic computing of having time ramp voltages to improve the energy efficiency as well as reliability. Figure 7.1 shows the schematic of the proposed adiabatic logic based PUF cell. The proposed adiabatic PUF cells consists of the cross coupled inverter (M1, M2, M3 and M4) similar to the memory based PUF. Further, the proposed adiabatic PUF cell also consists of a sleep transistor to enable or disable the PUF cell. When $\overline{enable}/disable$ is "1", the adiabatic PUF cell will be at the idle state (no operation will be performed). Figure 7.2 shows the time ramp voltage or the power clock ($V_{pc}$) voltage which is used to charge and discharge the output nodes in the proposed adiabatic PUF cell.

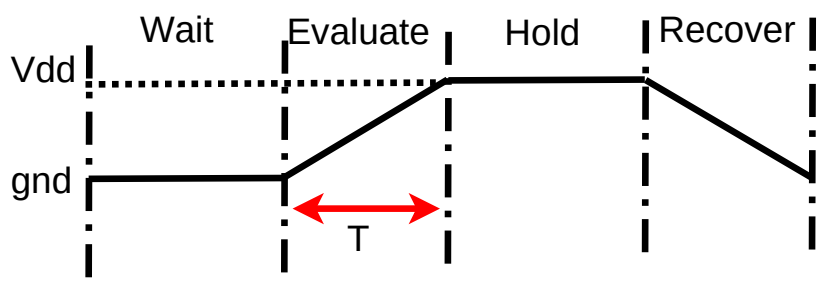



Figure 7.2: Time ramp voltage or power clock ($V_{pc}$) which is used in the proposed adiabatic PUF cell.

### 7.1.1 Operation of the proposed adiabatic logic based PUF cell

The operation of the proposed adiabatic logic based PUF cell through different phases of the clock (wait, evaluate, hold and recover) is explained below. Let us assume that disable is "0", so the MN0 transistor will be turned ON for the whole operation.

#### Wait Phase

During the wait phase, power clock ($V_{pc}$) will be at gnd. So, the PUF cell will be at idle state at this phase.

#### Evaluate phase

During the evaluate phase of $V_{pc}$, the $V_{pc}$ will slowly rise from gnd to $V_{dd}$. When $V_{pc}$ starts rising from gnd, both M1 and M2 transistors starts conducting. Due to the imperfections in the manufacturing process, both the transistors will have different threshold voltages. The transistor which has the lower threshold voltage conducts the current quickly as compared to the other and the corresponding load capacitor will quickly get charged. This leads to the flip in the outputs where one of the outputs leads to logic "1" and other to logic "0". For example, let us assume that the threshold voltage of M2 is greater than the threshold voltage of M1. Since the threshold voltage of M2 is greater than M1, the resistance of M2 will be greater than M1. When $V_{pc}$ is greater than $V_{tp}$, both M1 and M2 are turned ON. Since $R_{M2} > R_{M1}$, the output load capacitor will be charged quicker through M1

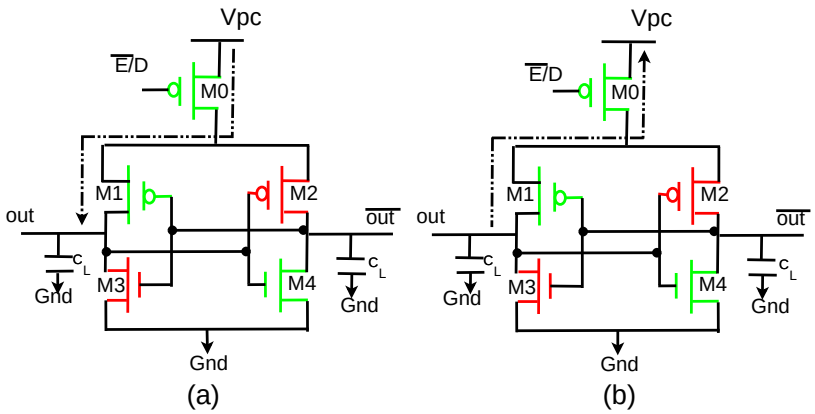



Figure 7.3: Operation of the proposed adiabatic PUF during a) Evaluate phase, b) Recover phase.

compared to $\overline{out}$ load capacitor. The operation of the proposed adiabatic logic PUF cell during the evaluate phase is shown in Figure 7.3 (a).

### Hold Phase

During the hold phase of the $V_{pc}$, the proposed adiabatic PUF will have stable PUF response.

### Recover phase

During the recover phase of the clock, the time ramp voltage is slowly reduced from $V_{dd}$ to gnd. During this phase, the charge stored in the load capacitor is slowly recovered back to the power clock generator circuit through the M1 transistor. Figure 7.3 (b) shows the operation of the proposed adiabatic PUF cell during the recover phase of the clock. Further, it has to be noted that the redundant voltage will be stored at the out node since M1 will be turned OFF when Vpc reaches $Vdd - V_{th}$. However, the redundant voltage ($V_{tp}$) will be useful to bias the PUF cell towards a constant logic“1” or logic “0” in the consecutive cycle of $V_{pc}$.

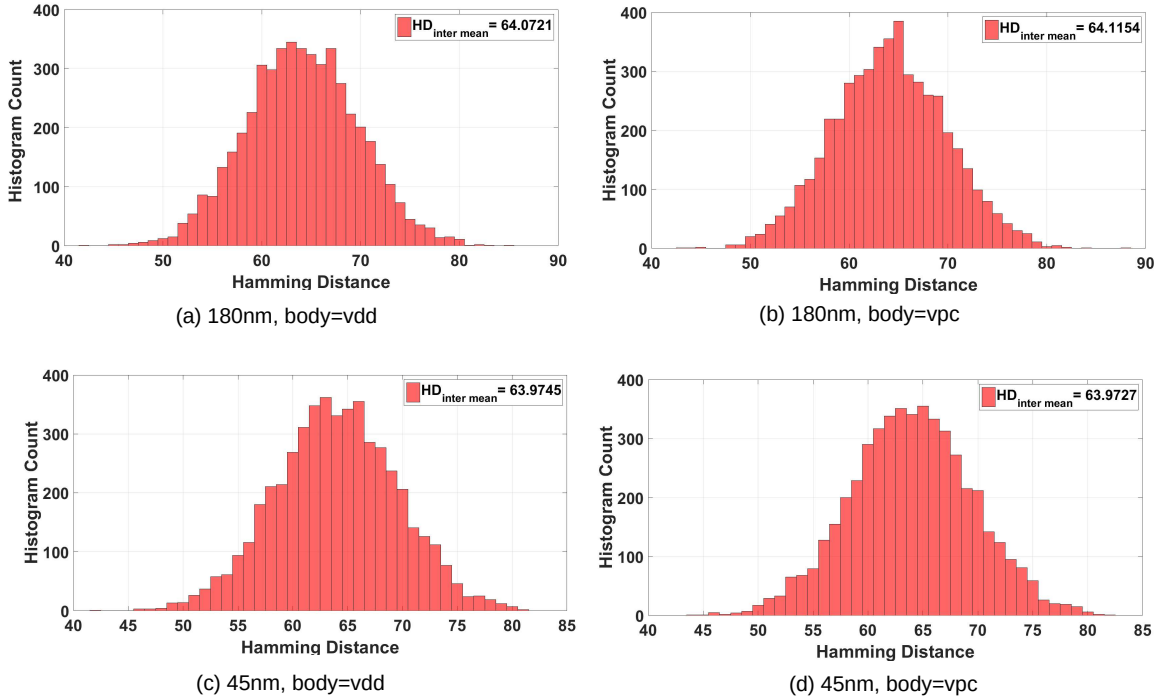



Figure 7.4: Inter-chip Hamming distance (HD) variations of the proposed 128 $\times$ 100 PUF at different CMOS technology and with body of PMOS connected to $V_{dd}$ and $V_{pc}$

## 7.2 Simulation results

To analyze the reproducibility of the proposed adiabatic logic PUF, we have designed and implemented a 128 bit PUF in a standard 180nm CMOS technology and simulated using Cadence Spectre simulator. Further, the evaluation of the proposed adiabatic PUF is also presented in 45nm CMOS technology. Simulation environments and the experiments are described in this section. Finally, the simulation results are presented.

### 7.2.1 Proposed PUF response

Each bit of the proposed adiabatic logic based PUF response is generated from the individual adiabatic logic based PUF cell. The major application of the proposed adiabatic PUF cell is to generate the key for the cryptographic operations, so we have implemented a 128 bit PUF array. In order to emulate the characterization of 100 IC PUF chips, 100 runs of Monte-Carlo simulation were performed.

In our simulations, temperature is varied from -40°C to 80°C with 27°C as the reference temperature. Further, we have also analyzed the reliability of the proposed adiabatic PUF by varying the peak power clock voltages by $\pm 20\% V_{dd}$.

### 7.2.2 Simulation environment and experiments

All simulations reported in this dissertation are performed using Cadence Spectre simulator. The transient noise is added through the simulation tool. The following parameters are considered for the proposed adiabatic PUF.

#### Body effect

In order to consider the body effect, we have simulated all the designs by connecting the body of the PMOS to $V_{dd}$ (constant voltage) and to $V_{pc}$ (power clock).

#### Temperature variation

In order to consider the temperature variations, we have varied the temperature from -40°C to 80°C. Simulations were performed at -40°C,-20°C,0°C,20°C,27°C,40°C,60°C, and 80°C.

#### Supply variation

We have varied the supply voltage variation by $\pm 20\%$ of the peak voltage of $V_{pc}$.

#### Technology parameters

In this work, we have considered the variation of PUF metrics by simulating the circuits at two different technology nodes. The channel lengths of the transistors play a major role in controlling manufacturing variations. So, in this research, we consider 180nm CMOS technology (long-channel) and 45nm CMOS technology (short-channel) to analyze the impact

of channel length variations. In first case, we presented all the values at 180nm CMOS technology and in the second case, we presented the PUF metrics when the circuit is simulated with 45nm CMOS technology.

Table 7.1: Simulated and calculated results of uniqueness($\%$) for the proposed $128 \times 100$ adiabatic PUF.

| Technology | Body | $HD_{inter-mean}$ | uniqueness($\%$) |
|---|---|---|---|
| 180nm | Vdd | 64.0721 | 49.5607 |
| 180nm | Vpc | 64.1154 | 49.5706 |
| 45nm | Vdd | 63.9743 | 49.4796 |
| 45nm | Vpc | 63.9727 | 49.4839 |

### 7.2.3 Simulation results and analysis

The simulation results and the analysis are presented in this section.

#### Uniqueness

Figure 7.4 shows the inter-chip Hamming Distance (HD) of the proposed $128 \times 100$ adiabatic PUF at 180nm CMOS technology and 45nm CMOS technology. Figure 7.4 (a) and (b) shows the inter chip HD of the proposed adiabatic PUF at 180nm CMOS technology with the body of PMOS connected to $V_{dd}$ and $V_{pc}$ respectively. Similarly, Figure 7.4 (c) and (d) shows the inter chip HD of the proposed adiabatic PUF at 45nm CMOS technology with the body of PMOS connected to $V_{dd}$ and $V_{pc}$ respectively. For the calculation purposes, we use the read response values of the proposed adiabatic PUF at the end of recovery phase. Based on the responses collected from 100 PUF instances, with each providing 128 bits, the mean inter chip HD value ($HD_{inter-mean}$)of the proposed $128 \times 100$ adiabatic PUF at 180nm CMOS technology when the body is connected to $V_{dd}$ is 64.0721 while when the body is connected to $V_{pc}$, $HD_{inter-mean}$ value is 64.1154. Similarly, $HD_{inter-mean}$ value of the proposed adiabatic PUF with the body connected to $V_{dd}$ and $V_{pc}$ is 63.9745 and 63.9727 respectively.

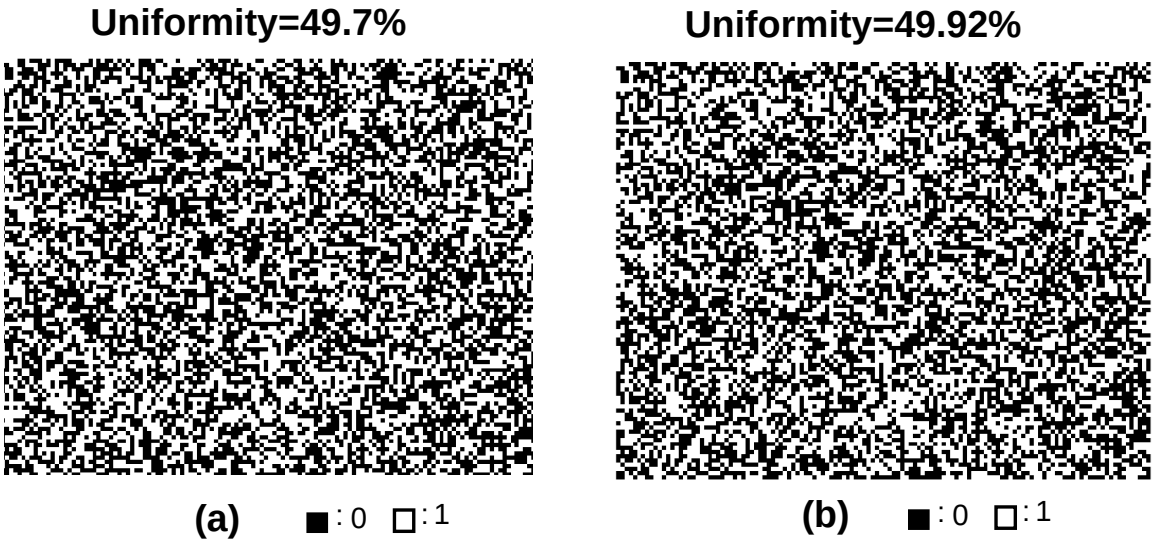



Figure 7.5: Gray scale bitmap showing the response of the proposed $128 \times 100$ adiabatic PUF at 180nm CMOS technology when the body of the PMOS devices connected to a) $V_{dd}$ and b)$V_{pc}$. Black pixel represents bit 0 and white pixel represents bit 1.

From the simulation results and calculations, we found that the uniqueness value of the proposed $128 \times 100$ adiabatic PUF at 180nm CMOS technology with body of PMOS connected to $V_{dd}$ is 49.5607% and to $V_{pc}$ is 49.5706%. Similarly, the uniqueness value of the proposed $128 \times 100$ adiabatic PUF at 45nm CMOS technology with body of PMOS connected to $V_{dd}$ is 49.4796% to $V_{pc}$ is 49.4839%. The ideal value of uniqueness is 50%. Table 7.1 summarizes the uniqueness result of the proposed adiabatic PUF at different CMOS technology.

**Uniformity**

Figures 7.5 (a) and (b) show the gray scale bit map image of the proposed $128 \times 100$ adiabatic PUF simulated at 180nm with body of the PMOS connected to $V_{dd}$ and $V_{pc}$ respectively. Similarly, Figures 7.6 (a) and (b) show the gray scale bit map image of the proposed 128 bit adiabatic PUF with 100 instances simulated at 45nm CMOS technology with body of the PMOS connected to $V_{dd}$ and $V_{pc}$ respectively. From the simulation results and calculations, the uniformity of the proposed adiabatic PUF at 180nm CMOS technol-

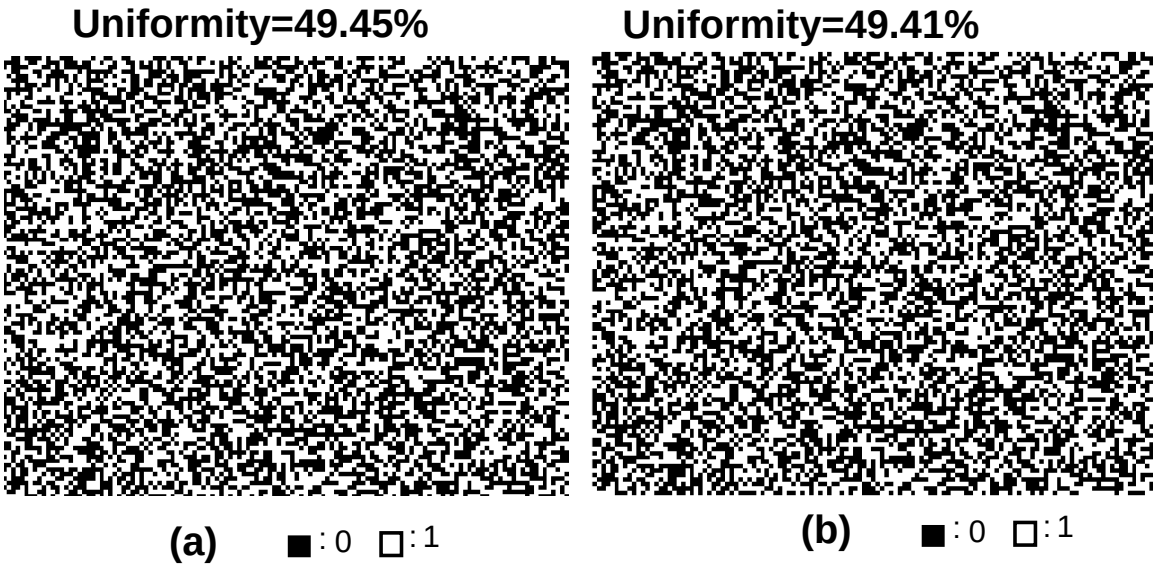



Figure 7.6: Gray scale bitmap showing the response of the proposed 128 $\times$ 100 adiabatic PUF at 45nm technology when the body of the PMOS devices connected to a) $V_{dd}$ and b) $V_{pc}$. Black pixel represents bit 0 and white pixel represents bit 1.

ogy with the body of PMOS connected to $V_{dd}$ is 49.7%. The uniformity of the proposed adiabatic PUF at 180nm CMOS technology with the body of PMOS connected to $V_{pc}$ is 49.92%. Similarly, the uniformity of the proposed adiabatic PUF at 45nm CMOS technology with the body of the PMOS connected to $V_{dd}$ is 49.45% and the uniformity of the PUF at 45nm with the body of the PMOS connected to $V_{pc}$ is 49.41%. As the probability of generating ones is close to ideal value of 50%, it indicates that the proposed adiabatic PUF output is not predictable and makes it hard to attack. Table 7.2 shows the uniformity results of the proposed adiabatic PUF with different configurations.

Table 7.2: Simulated and calculated results of uniformity(%) for the proposed 128 $\times$ 100 adiabatic PUF.

| Technology | Body | uniformity(%) |
|---|---|---|
| 180nm | Vdd | 49.7 |
| 180nm | Vpc | 49.92 |
| 45nm | Vdd | 49.45 |
| 45nm | Vpc | 49.41 |

**Reliability**

We have evaluated the reliability of the proposed adiabatic PUF by varying the temperature from -40°C to 80°C with 27°C as the reference temperature. Further we also evaluated the variation of supply voltage by varying the peak power clock voltage by $V_{dd}\pm 20\% V_{dd}$. Figure 7.7 shows reliability of the proposed adiabatic PUF against temperature variations for all the configurations of the proposed adiabatic PUF simulated at 180nm and 45nm CMOS technology.

**Reliability of proposed PUF at 180nm CMOS technology:** The average reliability of the proposed 128 bit adiabatic PUF with 100 instances at 180nm CMOS technology with body of PMOS connected to $V_{dd}$ is 97.7511% while with body of PMOS connected to $V_{pc}$ is 98.2109%. The worst case reliability of the proposed adiabatic PUF at 180nm CMOS technology when the body is connected to $V_{dd}$ and $V_{pc}$ is 96.3750% at 80°C and 96.8438 at 80°C respectively. Table 7.3 summarizes the average reliability of the proposed adiabatic PUF at different CMOS technologies and at different configurations.

**Reliability of proposed PUF at 45nm CMOS technology:** The average reliability of the proposed 128 bit adiabatic PUF with 100 instances at 45nm CMOS technology with body of PMOS connected to $V_{dd}$ is 99.5368%, while with body of PMOS connected to $V_{pc}$ is 99.7588%. The worst case reliability for the proposed adiabatic PUF at 45nm CMOS technology when the body is connected to $V_{dd}$ and $V_{pc}$ is 99.3281% at 60°C and 99.6016% at -40°C respectively. From our simulations and calculations, it is concluded that the proposed adiabatic PUF at 45nm CMOS technology has high reliability as compared to the 180nm CMOS technology.

**Reliability of proposed PUF against supply voltage variations:** Further, we have also evaluated the reliability of the proposed adiabatic PUF against supply voltage variations. The 100 PUF instances were simulated under different supply voltages from 0.8 to 1.2 V for 45nm CMOS technology and 1.6 to 2 V for 180nm CMOS technology and at three different temperatures, -40°C, 27°C, and 80°C. Reading the responses at the supply voltage

Table 7.3: Simulated and calculated results of average and worst case reliability(%) of the proposed $128 \times 100$ adiabatic PUF against temperature variations.

| Technology | Body | Average (%) | worst case (%) |
|---|---|---|---|
| 180nm | Vdd | 97.7511 | 96.3750 |
| 180nm | Vpc | 98.2109 | 96.8438 |
| 45nm | Vdd | 99.5368 | 99.3281 |
| 45nm | Vpc | 99.7588 | 99.6016 |

of 1.8 V for 180nm technology and 1 V for 45nm technology as reference, Bit Error Rate (BER) is calculated. Reliability can also calculated as be expressed in terms of Bit Error Rate (BER).

BER is expressed as,

$$BER\% = 100 - Reliability\% \tag{7.1}$$

Figures 7.8 (a) and (b) shows the BER of the proposed 128 bit adiabatic PUF when simulated at 180nm CMOS technology with body connected to $V_{dd}$ and $V_{pc}$ respectively. From the simulation results, we found that the worst case BER for 180nm CMOS technology is less than 6.2% and 6% when the body of PMOS connected to $V_{dd}$ and $V_{pc}$ respectively. Similarly, Figure 7.9 (a) and (b) shows the BER of the proposed 128 bit adiabatic PUF when simulated at 45nm CMOS technology with body connected to $V_{dd}$ and $V_{pc}$. From our simulation results, we found that the worst case BER is less than 0.36% when the body is connected to $V_{dd}$ while the BER is less than 0.42% when the body is connected to $V_{dd}$ and $V_{pc}$ respectively.

**Energy consumption**

Energy consumption is a very important parameter in the design of resource constrained devices. Table 7.4 provides the energy consumption comparison of the proposed adiabatic PUF along with the state-of-art PUFs. From Table 7.4, we can see that the proposed adi-

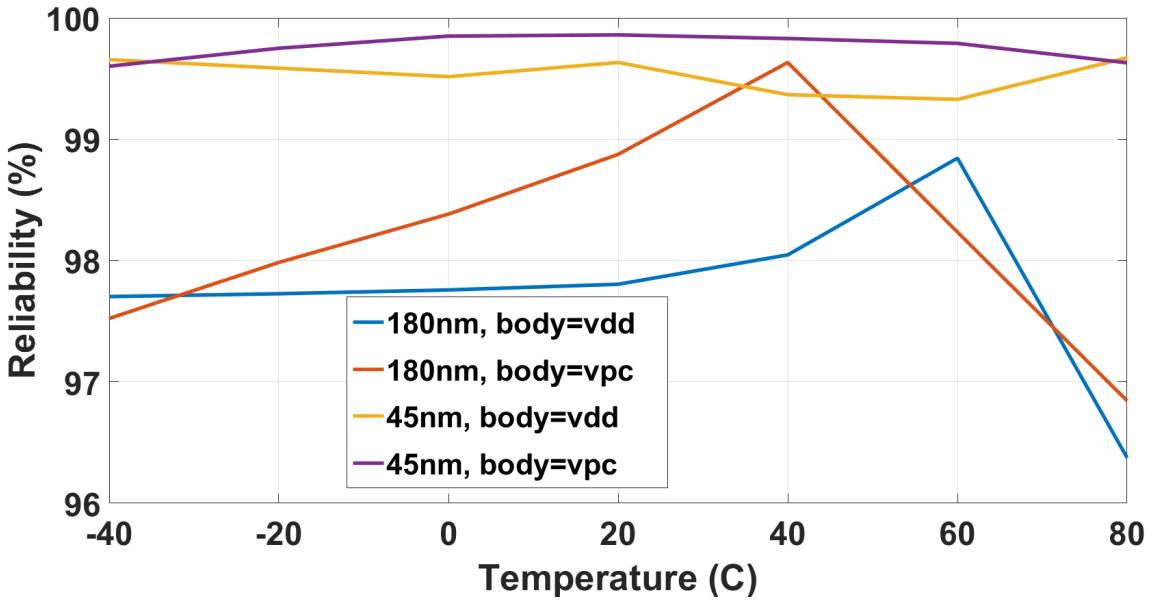



Figure 7.7: Reliability of the proposed adiabatic PUF with the change in temperature at different technology nodes and with body effect.

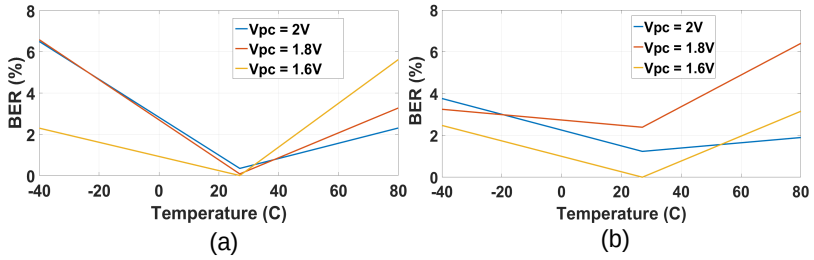



Figure 7.8: Bit Error Rate (BER) of the proposed adiabatic PUF with the supply voltage variation at 180nm CMOS technology with PMOS connected to a) $V_{dd}$, b) $V_{pc}$.

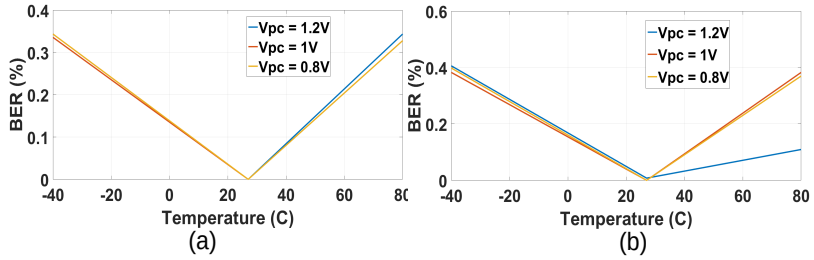



Figure 7.9: Bit Error Rate (BER) of the proposed adiabatic PUF with the supply voltage variation at 45nm CMOS technology with PMOS connected to a) $V_{dd}$, b) $V_{pc}$.

abatic PUF is energy efficient as compared to the PUFs listed in the Table 7.4. However, it has to be noted that the proposed adiabatic PUF has more energy consumption than [59] because the PUF proposed in [59] is operated at lower technology node and lower voltage than the proposed adiabatic PUF.

Table 7.4: Energy consumption comparison of the proposed adiabatic PUF with the state-of-art PUFs.

| PUF | Tech. | Vdd | Energy/bit |
|---|---|---|---|
| Lim et. al [41] | 180nm | 1.8 V | 1.37 pJ |
| Stanzione et. al [67] | 90nm | 1.2 V | 3.8 pJ |
| Majzoobi et. al [45] | 90nm | 1.2 V | 15 fJ |
| Cao et. al [16] | 180nm | 3.3 V | 23.9 pJ |
| Yang et. al [86] | 40nm | 0.9 V | 17.75 pJ |
| Neale et. al [59] | 28nm | 0.6 V | 0.045 fJ |
| Tao et. al [71] | 65nm | 0.6 V | 10.3 fJ |
| Proposed (This work) | 180nm | 1.8 V | 1.071 fJ |
| Proposed (This work) | 45nm | 1 V | 0.08 fJ |

Table 7.5: Security metric comparison of the proposed adiabatic PUF with the state-of-art PUFs.

| **PUF** | **Tech.** | **Vdd** | **Uniqu-eness** | **Uniformity** | **Reliability (worst case)** | **Energy /bit** |
|---|---|---|---|---|---|---|
| Lim et. al [41] | 180nm | 1.8 V | NA | NA | 95.18% | 1.37 pJ |
| Stanzione et. al [67] | 90nm | 1.2 V | NA | NA | 99.9% | 3.8 pJ |
| Majzoobi et. al [45] | 90nm | 1.2 V | NA | NA | 97% | 15 fJ |
| Cao et. al [16] | 180nm | 3.3 V | 49.37 % | NA | 99.1 % | 23.9 pJ |
| Yang et. al [86] | 40nm | 0.9 V | 47.22 % | NA | $\geq$ 99.99 % | 17.8 pJ |
| Neale et. al [59] | 28nm | 0.6 V | 49.11 % | 49.96 % | 88.39 | 0.05 fJ |
| Tao et. al [71] | 65nm | 0.6 V | 50.04 % | 49.5 % | 98.56 % | 10.3 fJ |
| Proposed (This work) | 180nm | 1.8 V | 49.97 % | 49.92 % | 96.84 % | 1.1 fJ |
| Proposed (This work) | 45nm | 1 V | 49.48 % | 49.41 % | 99.60 % | 0.08 fJ |

## 7.3 Discussion

In this research, we have employed adiabatic logic for several reasons to design the PUF circuit. Adiabatic logic technique is used to achieve low power and low energy consumption compared to the conventional CMOS circuits.

We designed a adiabatic logic based PUF to generate the secure key for the cryptographic systems in IoT devices. However, the reliability of the PUF is an important parameter to consider while designing the PUF to generate the reliable keys. Cortez et. al [21] has reported that intelligent choosing of time ramp up at a particular temperature can improve the reliability of SRAM PUF cells. However, this technique requires additional circuitry to perform the intelligent time ramp up operation to improve the reliability of SRAM PUF cell. Similarly, A. Vijayakumar et al. [80] have proposed a majority voting technique to improve the reliability of the SRAM PUF. However, this technique requires multiple turning on and turning off of the SRAM cell which results in additional power consumption.

In our adiabatic logic based PUF, time ramp voltages are used to recover the charge thereby reducing the energy consumption. Moreover, the usage of time ramp voltages is also used to improve the reliability of the proposed adiabatic PUF as discussed in [21]. The adiabatic clock can be generated as discussed in [6]. Further, it is to be noted that the adiabatic clock generator circuit will also be used to drive the cryptographic processor in the circuit to improve the energy-efficiency.

### 7.3.1 Security metric comparison of proposed adiabatic PUF with state-of-art PUFs

Table 7.5 provides the security metric comparison with the proposed adiabatic PUF. All the data reported here are obtained from the corresponding paper. NA in the table represents data not available. From Table 7.5, we can see that the PUF proposed in [41] using 180nm technology with 1.8 V has the worst case reliability of 95.18% with 1.37 pJ of energy con-

sumption per bit. Our proposed adiabatic PUF which is simulated in 180nm technology has the worst case reliability of 96.84% with the 1.071 fJ of energy consumption per bit per cycle. However, PUF proposed in [17] using 180nm CMOS technology has better worst case reliability than the proposed adiabatic PUF, while consuming 23.9 pJ of energy/bit. The PUF proposed in [67] using 90nm CMOS technology has 99.99% of worst case reliability consuming 3.8pJ/bit of energy. The PUF proposed in [45] using 90nm CMOS technology has lower reliability than PUF proposed in [67] consuming lower energy.

Similarly, the PUF proposed in [86] has very high reliability of 99.99% but suffers from high energy consumption which makes it not suitable to implement in IoT devices. Our proposed adiabatic PUF at 45nm CMOS technology has a worst case reliability of 99.68 % with very low energy consumption. High reliability, low energy consumption and low implementation cost make the proposed adiabatic PUF a suitable candidate for IoT devices and medical devices. The proposed adiabatic PUF in 45nm CMOS technology has more energy consumption than [59] because the PUF proposed in [59] is operated at lower technology node and lower voltage than the proposed adiabatic PUF. However, reliability of the PUF in [59] is 88.39% which makes them not suitable to generate reliable key for IoT devices.

## 7.4 Summary

A low cost adiabatic logic based CMOS PUF that generates unique and reliable response bits have been proposed and evaluated. The proposed adiabatic logic based PUF uses the time ramp voltages to recover the charge from the load capacitor to achieve energy efficiency as well as improve the reliability. From our simulation results, we observed that the proposed adiabatic PUF at 180nm CMOS technology and 45nm CMOS technology has the uniqueness and uniformity values close to the ideal value of 50%. The reliability of the PUF is also verified by varying the temperature from -40°C to 80°C and also by varying

the supply voltage by $\pm 20\%$ $V_{dd}$. Moreover, the proposed adiabatic PUF has significant energy savings as compared to the existing PUFs. Low energy consumption per bit, high reliability, close to ideal uniqueness and uniformity values make our adiabatic PUF a suitable candidate to implement in battery operated IoT devices. Some of the applications of our proposed PUF include secure key generation, device authentication, memoryless key storage, Intellectual Property (IP) protection etc.

# Chapter 8

# Conclusion and Future Directions

Internet of Things (IoT) is a network of devices that are connected through the Internet to exchange data for intelligent applications. Though IoT devices provide several advantages to improve the quality of life, they also equally present challenges related to security and piracy. The security issues in IoT devices include leakage of information through Differential Power Analysis (DPA) based side channel attacks, authentication, piracy, etc. Improvement in the security of IoT devices comes at the cost of reduction in battery life. IoT devices are battery operated, therefore this dissertation explores research solutions to hardware security and power consumption problems in IoT devices with novel circuit design techniques in emerging transistors and non-volatile memories.

Our first contribution is the proposal of a novel DPA-resistant adiabatic logic family called Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL). EE-SPFAL based circuits are energy-efficient compared to the existing DPA-resistant adiabatic logic achieved by reducing the non-adiabatic energy loss during the switching of input data. Further, EE-SPFAL based circuits consume uniform power irrespective of input data transition which makes them resilience against DPA attacks. Along with the low-power circuit design methodologies, various low-leakage emerging devices have been investigated to address the power budget issue in IoT devices.

In the second contribution of this dissertation, we have investigated the usefulness of FinFET device along with adiabatic logic in the design of DPA secure hardware. As a result, we have proposed a novel FinFET based Secure Adiabatic Logic (FinSAL) family. FinSAL based designs utilize low-leakage FinFET device along with adiabatic logic principles to improve energy-efficiency along with its resistance against DPA attack.

In the third contribution of this dissertation, we have explored the usefulness of designing MTJ/CMOS based cryptographic circuits and evaluated its resilience against the DPA attack. As a result we have proposed a novel approach of building cryptographic hardware in MTJ/CMOS circuits using Look-Up Table (LUT) based method where the data stored in MTJs are constant during the entire encryption/decryption operation. As a case study, we have implemented a S-box circuit and one round of the PRESENT-80 lightweight cryptographic algorithm using Look-Up Table (LUT) method. The proposed LUT method implementation in MTJ/CMOS has improved energy-efficiency and DPA resistance property compared to conventional CMOS based designs.

In the fourth contribution of this dissertation, we have proposed a novel energy-efficient Secure MTJ/CMOS Logic (SMCL) family. The proposed SMCL logic family consumes uniform power irrespective of data transition in MTJ and more energy-efficient as compared to the state-of-art MTJ/CMOS designs by using charge sharing technique.

The other important contribution of this dissertation is the design of reliable Physical Unclonable Function (PUF) using adiabatic logic technique. The time ramp voltages in adiabatic PUF are utilized to improve the reliability of PUF along with its energy-efficiency. Reliability of the adiabatic logic based PUF proposed in this dissertation is tested through simulation based temperature variations and supply voltage variations.

We also presented the low-power design techniques to address the power budget and the security problems in low-power IoT devices. The results presented in this dissertation have been obtained using the industry standard CAD tools such as Cadence Virtuoso, Cadence Assura, etc. As a future work of this research, practical evaluation of the designs will be

performed on the silicon prototyping. Adiabatic logic technique is a low-power design technique to design energy-efficient and secure hardware. These circuits utilizes multi-phase clocking to recover the charge. As a future directions, the proposed circuits can be integrated with wireless charging circuit in order to design energy-efficient wireless charging based DPA resistant hardware.

# References


[1] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[2] Massimo Alioto, Simone Bongiovanni, Milena Djukanovic, Gianmario Scotti, and Alessandro Trifiletti. Effectiveness of leakage power analysis attacks on dpa-resistant logic styles under process variations. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 61(2):429–442, 2014.

[3] Jude Angelo Ambrose, Sri Parameswaran, and Aleksandar Ignjatovic. Mute-aes: a multiprocessor architecture to prevent power analysis based side channel attack of the aes algorithm. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, pages 678–684. IEEE Press, 2008.

[4] Ross Anderson and Markus Kuhn. Low cost attacks on tamper resistant devices. In *International Workshop on Security Protocols*, pages 125–136. Springer, 1997.

[5] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, 1(2):99–109, 2015.

[6] Muhammad Arsalan and Maitham Shams. Charge-recovery power clock generators for adiabatic logic circuits. In *VLSI Design, 2005. 18th International Conference on*, pages 171–174. IEEE, 2005.

[7] William C Athas, Lars J Svensson, Jeffrey G Koller, Nestoras Tzartzanis, and Eric Ying-Chin Chou. Low-power digital systems based on adiabatic-switching principles. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 2(4):398–407, 1994.

[8] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[9] Moshe Avital, Hadar Dagan, Itamar Levi, Osnat Keren, and Alexander Fish. Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 62(1):149–156, 2015.

[10] Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69, 2011.

[11] Behtash Behin-Aein, Jian-Ping Wang, and Roland Wiesendanger. Computing with spins and magnets. *MRS Bulletin*, 39(08):696–702, 2014.

[12] D Blaauw, D Sylvester, P Dutta, Y Lee, I Lee, S Bang, Y Kim, G Kim, P Pannuto, Y-S Kuo, et al. Iot design space challenges: Circuits and systems. In *2014 Symposium on VLSI Technology (VLSI-Technology): Digest of Technical Papers*, pages 1–2. IEEE, 2014.

[13] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. Present: An ultra-lightweight block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 450–466. Springer, 2007.

[14] Marco Bucci, Luca Giancane, Raimondo Luzzi, Giuseppe Scotti, and Alessandro Trifiletti. Delay-based dual-rail precharge logic. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 19(7):1147–1153, 2011.

[15] Marco Bucci, Luca Giancane, Raimondo Luzzi, and Alessandro Trifiletti. Three-phase dual-rail pre-charge logic. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 232–241. Springer, 2006.

[16] Yuan Cao, Le Zhang, Chip-Hong Chang, and Shoushun Chen. A low-power hybrid ro puf with improved thermal stability for lightweight applications. *IEEE Transactions on computer-aided design of integrated circuits and systems*, 34(7):1143–1147, 2015.

[17] Yuan Cao, Le Zhang, Siarhei S Zalivaka, Chip-Hong Chang, and Shoushun Chen. Cmos image sensor based physical unclonable function for coherent sensor-level authentication. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 62(11):2629–2640, 2015.

[18] Qingqing Chen, György Csaba, Paolo Lugli, Ulf Schlichtmann, and Ulrich Rührmair. Characterization of the bistable ring puf. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 1459–1462. EDA Consortium, 2012.

[19] Byong-Deok Choi, Kyung Eun Kim, Ki-Seok Chung, and Dong Kyue Kim. Symmetric adiabatic logic circuits against differential power analysis. *ETRI journal*, 32(1):166–168, 2010.

[20] International Roadmap Committee et al. International technology roadmap for semiconductors, 2008.

[21] Mafalda Cortez, Said Hamdioui, Ali Kaichouhi, Vincent van der Leest, Roel Maes, and Geert-Jan Schrijen. Intelligent voltage ramp-up time adaptation for temperature noise reduction on memory-based puf systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(7):1162–1175, 2015.

[22] Erya Deng, Yue Zhang, Jacques-Olivier Klein, Dafiné Ravelsona, Claude Chappert, and Weisheng Zhao. Low power magnetic full-adder based on spin transfer torque mram. *IEEE transactions on magnetics*, 49(9):4982–4987, 2013.

[23] Jean-Francois Dhem, Francois Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, and Jean-Louis Willems. A practical implementation of the timing attack. In *Smart Card Research and Applications*, pages 167–182. Springer, 1998.

[24] Dave Evans. The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, 1(2011):1–11, 2011.

[25] Hsing-Ping Fu, Ju-Hung Hsiao, Po-Chun Liu, Hsie-Chia Chang, and Chen-Yi Lee. A low cost dpa-resistant 8-bit aes core based on ring oscillators. In *VLSI Design, Automation, and Test (VLSI-DAT), 2012 International Symposium on*, pages 1–4. IEEE, 2012.

[26] Yi Gang, Weisheng Zhao, Jacques-Olivier Klein, Claude Chappert, and Pascale Mazoyer. A high-reliability, low-power magnetic full adder. *IEEE Transactions on Magnetics*, 47(11):4611–4616, 2011.

[27] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

[28] Digh Hisamoto, Wen-Chin Lee, Jakub Kedzierski, Hideki Takeuchi, Kazuya Asano, Charles Kuo, Erik Anderson, Tsu-Jae King, Jeffrey Bokor, and Chenming Hu. Finfet-a self-aligned double-gate mosfet scalable to 20 nm. *Electron Devices, IEEE Transactions on*, 47(12):2320–2325, 2000.

[29] Daniel E Holcomb, Wayne P Burleson, and Kevin Fu. Power-up sram state as an identifying fingerprint and source of true random numbers. *Computers, IEEE Transactions on*, 58(9):1198–1210, 2009.

[30] Anirudh Srikant Iyengar. Energy-efficient and secure designs of spintronic memory: Techniques and applications. 2018.

[31] LIM Joonho, Kim Dong-Gyu, and CHAE Soo-Ik. Reversible energy recovery logic circuits and its 8-phase clocked power generator for ultra-low-power applications. *IEICE transactions on electronics*, 82(4):646–653, 1999.

[32] Wang Kang, Weifeng Lv, Youguang Zhang, and Weisheng Zhao. Low store power high-speed high-density nonvolatile sram design with spin hall effect-driven magnetic tunnel junctions. *IEEE Transactions on Nanotechnology*, 16(1):148–154, 2017.

[33] Wang Kang, Yue Zhang, Zhaohao Wang, Jacques-Olivier Klein, Claude Chappert, Dafiné Ravelosona, Gefei Wang, Youguang Zhang, and Weisheng Zhao. Spintronics: Emerging ultra-low-power circuits and systems beyond mos technology. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 12(2):16, 2015.

[34] Mehrdad Khatir and Amir Moradi. Secure adiabatic logic: a low-energy dpa-resistant logic style. *IACR Cryptology ePrint Archive*, 2008:123, 2008.

[35] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in CryptologyCRYPTO99*, pages 388–397. Springer, 1999.

[36] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27, 2011.

[37] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Ee-spfal: A novel energy-efficient secure positive feedback adiabatic logic for dpa resistant rfid and smart card. *IEEE Transactions on Emerging Topics in Computing*, 2016.

[38] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Finsal: A novel finfet based secure adiabatic logic for energy-efficient and dpa resistant iot devices. In *IEEE International Conference on Rebooting Computing*. IEEE, 2016. © 2016 IEEE Reprinted, with permission.

[39] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Finsal: Finfet-based secure adiabatic logic for energy-efficient and dpa resistant iot devices. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):110–122, 2018. © 2018 IEEE Reprinted, with permission.

[40] Klaus Kursawe, Dries Schellekens, and Bart Preneel. Analyzing trusted platform communication. In *ECRYPT Workshop, CRASH-CRyptographic Advances in Secure Hardware*, 2005.

[41] Daihyun Lim, Jae W Lee, Blaise Gassend, G Edward Suh, Marten Van Dijk, and Srinivas Devadas. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13(10):1200–1205, 2005.

[42] Joonho Lim, Kipaek Kwon, and Soo-Ik Chae. Reversible energy recovery logic circuit without non-adiabatic energy loss. *Electronics Letters*, 34(4):344–346, 1998.

[43] Shengshuo Lu, Zhengya Zhang, and Marios Papaefthymiou. 1.32 ghz high-throughput charge-recovery aes core with resistance to dpa attacks. In *2015 Symposium on VLSI Circuits (VLSI Circuits)*, pages C246–C247. IEEE, 2015.

[44] Denise Lund, Carrie MacGillivray, Vernon Turner, and Mario Morales. Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand. *International Data Corporation (IDC), Tech. Rep*, 2014.

[45] Mehrdad Majzoobi, Golsa Ghiaasi, Farinaz Koushanfar, and Sani R Nassif. Ultra-low power current-based puf. In *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*, pages 2071–2074. IEEE, 2011.

[46] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*, volume 31. Springer Science & Business Media, 2008.

[47] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. *Disruptive technologies: Advances that will transform life, business, and the global economy*, volume 180. McKinsey Global Institute San Francisco, CA, 2013.

[48] Cedric Marchand, Lilian Bossuet, Ugo Mureddu, Nathalie Bochard, Abdelkarim Cherkaoui, and Viktor Fischer. Implementation and characterization of a physical unclonable function for iot: a case study with the tero-puf. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2017.

[49] Thomas S Messerges, Ezzat A Dabbish, and Robert H Sloan. Examining smart-card security under the threat of power analysis attacks. *Computers, IEEE Transactions on*, 51(5):541–552, 2002.

[50] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan. Investigations of power analysis attacks on smartcards. *Smartcard*, 99:151–161, 1999.

[51] Câncio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine. Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level. *Microelectronics Journal*, 44(6):496–503, 2013.

[52] Câncio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine. Low-power secure s-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design. *IET Circuits, Devices & Systems*, 9(5):362–369, 2015.

[53] Jagadeesh Subbaiah Moodera, Lisa R Kinder, Terrilyn M Wong, and R Meservey. Large magnetoresistance at room temperature in ferromagnetic thin film tunnel junctions. *Physical review letters*, 74(16):3273, 1995.

[54] Yong Moon and Deog-Kyoon Jeong. An efficient charge recovery logic circuit. *IEEE journal of solid-state circuits*, 31(4):514–522, 1996.

[55] Amir Moradi and Axel Poschmann. Lightweight cryptography and dpa countermeasures: A survey. In *Financial Cryptography and Data Security*, pages 68–79. Springer, 2010.

[56] Amir Moradi, Mohammad Taghi Manzuri Shalmani, and Mahmoud Salmasizadeh. Dual-rail transition logic: A logic style for counteracting power analysis attacks. *Computers & Electrical Engineering*, 35(2):359–369, 2009.

[57] Sumio Morioka and Akashi Satoh. An optimized s-box circuit architecture for low power aes design. In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 172–186. Springer, 2002.

[58] Debdeep Mukhopadhyay. Pufs as promising tools for security in internet of things. *IEEE Design & Test*, 33(3):103–115, 2016.

[59] Adam Neale and Manoj Sachdev. A low energy sram-based physically unclonable function primitive in 28 nm cmos. In *Custom Integrated Circuits Conference (CICC), 2015 IEEE*, pages 1–4. IEEE, 2015.

[60] Thomas Popp and Stefan Mangard. Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 172–186. Springer, 2005.

[61] NIST FIPS Pub. 197: Advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197:441–0311, 2001.

[62] Fengbo Ren and Dejan Markovic. True energy-performance analysis of the mtj-based logic-in-memory architecture (1-bit full adder). *IEEE Transactions on Electron Devices*, 57(5):1023–1028, 2010.

[63] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of aes. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 413–427. Springer, 2010.

[64] Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents. In *International Conference on Smart Card Research and Advanced Applications*, pages 89–103. Springer, 2008.

[65] Carl A Schu, Daniel R Greeninger, and David L Thompson. Power dissipation reduction in medical devices using adiabatic logic, August 20 2002. US Patent 6,438,422.

[66] Sergei Petrovich Skorobogatov. *Semi-invasive attacks: a new approach to hardware security analysis*. PhD thesis, Citeseer, 2005.

[67] Stefano Stanzione, Daniele Puntin, and Giuseppe Iannaccone. Cmos silicon physical unclonable functions based on intrinsic process variability. *IEEE Journal of Solid-State Circuits*, 46(6):1456–1463, 2011.

[68] Ben G Streetman and Sanjay Banerjee. *Solid state electronic devices*, volume 4. Prentice Hall New Jersey, 2000.

[69] G Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual Design Automation Conference*, pages 9–14. ACM, 2007.

[70] Daisuke Suzuki, Minoru Saeki, and Tetsuya Ichikawa. Random switching logic: A new countermeasure against dpa and second-order dpa at the logic level. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 90(1):160–168, 2007.

[71] Sha Tao and Elena Dubrova. Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm cmos. *Electronics Letters*, 52(10):805–806, 2016.

[72] Philip Teichmann. *Adiabatic logic: future trend and system level perspective*, volume 34. Springer Science & Business Media, 2011.

[73] Himanshu Thapliyal, Fazel Sharifi, and S Dinesh Kumar. Energy-efficient design of hybrid mtj/cmos and mtj/nanoelectronics circuits. *IEEE Transactions on Magnetics*, 2018.

[74] Kris Tiri, Moonmoon Akmal, and Ingrid Verbauwhede. A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Solid-State Circuits Conference, 2002. ESSCIRC 2002. Proceedings of the 28th European*, pages 403–406. IEEE, 2002.

[75] Kris Tiri and Ingrid Verbauwhede. Charge recycling sense amplifier based logic: securing low power security ics against dpa. In *30th European Conference on Solid-State Circuits*, pages 179–182, 2004.

[76] Kris Tiri and Ingrid Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, page 10246. IEEE Computer Society, 2004.

[77] Wim Van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

[78] Anthony Van Herrewege. Lightweight puf-based key and random number generation. 2015.

[79] A Vetuli, S Di Pascoli, and LM Reyneri. Positive feedback in adiabatic logic. *Electronics Letters*, 32(20):1867–1868, 1996.

[80] Arunkumar Vijayakumar, Vinay C Patil, and Sandip Kundu. On improving reliability of sram-based physically unclonable functions. *Journal of Low Power Electronics and Applications*, 7(1):2, 2017.

[81] Tutu Wan, Yasha Karimi, Milutin Stanacevic, and Emre Salman. Energy efficient ac computing methodology for wirelessly powered iot devices. In *Circuits and Systems (ISCAS), 2017 IEEE International Symposium on*, pages 1–4. IEEE, 2017.

[82] Tutu Wan, Yasha Karimi, Milutin Stanaćević, and Emre Salman. Perspective papercan ac computing be an alternative for wirelessly powered iot devices? *IEEE Embedded Systems Letters*, 9(1):13–16, 2017.

[83] You WANG, Yue ZHANG, Jacques-Olivier Klein, Thibaut Devolder, Dafin Ravelosona, Claude Chappert, and Weisheng Zhao. Compact model for perpendicular magnetic anisotropy magnetic tunnel junction, Aug 2017.

[84] Marilyn Wolf. Ultralow power and the new era of not-so-vlsi. *IEEE Design & Test*, 33(4):109–113, 2016.

[85] Huapeng Wu. Bit-parallel finite field multiplier and squarer using polynomial basis. *IEEE Transactions on Computers*, 51(7):750–758, 2002.

[86] Kaiyuan Yang, Qing Dong, David Blaauw, and Dennis Sylvester. 14.2 a physically unclonable function with ber¡ 10- 8 for robust chip authentication using oscillator collapse in 40nm cmos. In *Solid-State Circuits Conference-(ISSCC), 2015 IEEE International*, pages 1–3. IEEE, 2015.

[87] Yibin Ye and Kaushik Roy. Qserl: Quasi-static energy recovery logic. *Solid-State Circuits, IEEE Journal of*, 36(2):239–248, 2001.

[88] Ramtin Zand, Arman Roohi, Soheil Salehi, and Ronald F DeMara. Scalable adaptive spintronic reconfigurable logic using area-matched mtj design. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 63(7):678–682, 2016.

[89] Yue Zhang, Weisheng Zhao, Yahya Lakys, Jacques-Olivier Klein, Joo-Von Kim, Dafiné Ravelosona, and Claude Chappert. Compact modeling of perpendicular-anisotropy cofeb/mgo magnetic tunnel junctions. *IEEE Transactions on Electron Devices*, 59(3):819–826, 2012.

[90] Weisheng Zhao, Mathieu Moreau, Erya Deng, Yue Zhang, Jean-Michel Portal, Jacques-Olivier Klein, Marc Bocquet, Hassen Aziza, Damien Deleruyelle, Christophe Muller, et al. Synchronous non-volatile logic gate design based on resistive switching memories. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(2):443–454, 2014.

# References


[1] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376, 2015.

[2] Massimo Alioto, Simone Bongiovanni, Milena Djukanovic, Gianmario Scotti, and Alessandro Trifiletti. Effectiveness of leakage power analysis attacks on dpa-resistant logic styles under process variations. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 61(2):429–442, 2014.

[3] Jude Angelo Ambrose, Sri Parameswaran, and Aleksandar Ignjatovic. Mute-aes: a multiprocessor architecture to prevent power analysis based side channel attack of the aes algorithm. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, pages 678–684. IEEE Press, 2008.

[4] Ross Anderson and Markus Kuhn. Low cost attacks on tamper resistant devices. In *International Workshop on Security Protocols*, pages 125–136. Springer, 1997.

[5] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, 1(2):99–109, 2015.

[6] Muhammad Arsalan and Maitham Shams. Charge-recovery power clock generators for adiabatic logic circuits. In *VLSI Design, 2005. 18th International Conference on*, pages 171–174. IEEE, 2005.

[7] William C Athas, Lars J Svensson, Jeffrey G Koller, Nestoras Tzartzanis, and Eric Ying-Chin Chou. Low-power digital systems based on adiabatic-switching principles. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 2(4):398–407, 1994.

[8] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[9] Moshe Avital, Hadar Dagan, Itamar Levi, Osnat Keren, and Alexander Fish. Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 62(1):149–156, 2015.

[10] Debasis Bandyopadhyay and Jaydip Sen. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1):49–69, 2011.

[11] Behtash Behin-Aein, Jian-Ping Wang, and Roland Wiesendanger. Computing with spins and magnets. *MRS Bulletin*, 39(08):696–702, 2014.

[12] D Blaauw, D Sylvester, P Dutta, Y Lee, I Lee, S Bang, Y Kim, G Kim, P Pannuto, Y-S Kuo, et al. Iot design space challenges: Circuits and systems. In *2014 Symposium on VLSI Technology (VLSI-Technology): Digest of Technical Papers*, pages 1–2. IEEE, 2014.

[13] Andrey Bogdanov, Lars R Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew JB Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. Present: An ultra-lightweight block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 450–466. Springer, 2007.

[14] Marco Bucci, Luca Giancane, Raimondo Luzzi, Giuseppe Scotti, and Alessandro Trifiletti. Delay-based dual-rail precharge logic. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 19(7):1147–1153, 2011.

[15] Marco Bucci, Luca Giancane, Raimondo Luzzi, and Alessandro Trifiletti. Three-phase dual-rail pre-charge logic. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 232–241. Springer, 2006.

[16] Yuan Cao, Le Zhang, Chip-Hong Chang, and Shoushun Chen. A low-power hybrid ro puf with improved thermal stability for lightweight applications. *IEEE Transactions on computer-aided design of integrated circuits and systems*, 34(7):1143–1147, 2015.

[17] Yuan Cao, Le Zhang, Siarhei S Zalivaka, Chip-Hong Chang, and Shoushun Chen. Cmos image sensor based physical unclonable function for coherent sensor-level authentication. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 62(11):2629–2640, 2015.

[18] Qingqing Chen, György Csaba, Paolo Lugli, Ulf Schlichtmann, and Ulrich Rührmair. Characterization of the bistable ring puf. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 1459–1462. EDA Consortium, 2012.

[19] Byong-Deok Choi, Kyung Eun Kim, Ki-Seok Chung, and Dong Kyue Kim. Symmetric adiabatic logic circuits against differential power analysis. *ETRI journal*, 32(1):166–168, 2010.

[20] International Roadmap Committee et al. International technology roadmap for semiconductors, 2008.

[21] Mafalda Cortez, Said Hamdioui, Ali Kaichouhi, Vincent van der Leest, Roel Maes, and Geert-Jan Schrijen. Intelligent voltage ramp-up time adaptation for temperature noise reduction on memory-based puf systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 34(7):1162–1175, 2015.

[22] Erya Deng, Yue Zhang, Jacques-Olivier Klein, Dafiné Ravelsona, Claude Chappert, and Weisheng Zhao. Low power magnetic full-adder based on spin transfer torque mram. *IEEE transactions on magnetics*, 49(9):4982–4987, 2013.

[23] Jean-Francois Dhem, Francois Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, and Jean-Louis Willems. A practical implementation of the timing attack. In *Smart Card Research and Applications*, pages 167–182. Springer, 1998.

[24] Dave Evans. The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, 1(2011):1–11, 2011.

[25] Hsing-Ping Fu, Ju-Hung Hsiao, Po-Chun Liu, Hsie-Chia Chang, and Chen-Yi Lee. A low cost dpa-resistant 8-bit aes core based on ring oscillators. In *VLSI Design, Automation, and Test (VLSI-DAT), 2012 International Symposium on*, pages 1–4. IEEE, 2012.

[26] Yi Gang, Weisheng Zhao, Jacques-Olivier Klein, Claude Chappert, and Pascale Mazoyer. A high-reliability, low-power magnetic full adder. *IEEE Transactions on Magnetics*, 47(11):4611–4616, 2011.

[27] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, and Srinivas Devadas. Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, 2014.

[28] Digh Hisamoto, Wen-Chin Lee, Jakub Kedzierski, Hideki Takeuchi, Kazuya Asano, Charles Kuo, Erik Anderson, Tsu-Jae King, Jeffrey Bokor, and Chenming Hu. Finfet-a self-aligned double-gate mosfet scalable to 20 nm. *Electron Devices, IEEE Transactions on*, 47(12):2320–2325, 2000.

[29] Daniel E Holcomb, Wayne P Burleson, and Kevin Fu. Power-up sram state as an identifying fingerprint and source of true random numbers. *Computers, IEEE Transactions on*, 58(9):1198–1210, 2009.

[30] Anirudh Srikant Iyengar. Energy-efficient and secure designs of spintronic memory: Techniques and applications. 2018.

[31] LIM Joonho, Kim Dong-Gyu, and CHAE Soo-Ik. Reversible energy recovery logic circuits and its 8-phase clocked power generator for ultra-low-power applications. *IEICE transactions on electronics*, 82(4):646–653, 1999.

[32] Wang Kang, Weifeng Lv, Youguang Zhang, and Weisheng Zhao. Low store power high-speed high-density nonvolatile sram design with spin hall effect-driven magnetic tunnel junctions. *IEEE Transactions on Nanotechnology*, 16(1):148–154, 2017.

[33] Wang Kang, Yue Zhang, Zhaohao Wang, Jacques-Olivier Klein, Claude Chappert, Dafiné Ravelosona, Gefei Wang, Youguang Zhang, and Weisheng Zhao. Spintronics: Emerging ultra-low-power circuits and systems beyond mos technology. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 12(2):16, 2015.

[34] Mehrdad Khatir and Amir Moradi. Secure adiabatic logic: a low-energy dpa-resistant logic style. *IACR Cryptology ePrint Archive*, 2008:123, 2008.

[35] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in CryptologyCRYPTO99*, pages 388–397. Springer, 1999.

[36] Paul Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27, 2011.

[37] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Ee-spfal: A novel energy-efficient secure positive feedback adiabatic logic for dpa resistant rfid and smart card. *IEEE Transactions on Emerging Topics in Computing*, 2016.

[38] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Finsal: A novel finfet based secure adiabatic logic for energy-efficient and dpa resistant iot devices. In *IEEE International Conference on Rebooting Computing*. IEEE, 2016. © 2016 IEEE Reprinted, with permission.

[39] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Finsal: Finfet-based secure adiabatic logic for energy-efficient and dpa resistant iot devices. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):110–122, 2018. © 2018 IEEE Reprinted, with permission.

[40] Klaus Kursawe, Dries Schellekens, and Bart Preneel. Analyzing trusted platform communication. In *ECRYPT Workshop, CRASH-CRyptographic Advances in Secure Hardware*, 2005.

[41] Daihyun Lim, Jae W Lee, Blaise Gassend, G Edward Suh, Marten Van Dijk, and Srinivas Devadas. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13(10):1200–1205, 2005.

[42] Joonho Lim, Kipaek Kwon, and Soo-Ik Chae. Reversible energy recovery logic circuit without non-adiabatic energy loss. *Electronics Letters*, 34(4):344–346, 1998.

[43] Shengshuo Lu, Zhengya Zhang, and Marios Papaefthymiou. 1.32 ghz high-throughput charge-recovery aes core with resistance to dpa attacks. In *2015 Symposium on VLSI Circuits (VLSI Circuits)*, pages C246–C247. IEEE, 2015.

[44] Denise Lund, Carrie MacGillivray, Vernon Turner, and Mario Morales. Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand. *International Data Corporation (IDC), Tech. Rep*, 2014.

[45] Mehrdad Majzoobi, Golsa Ghiaasi, Farinaz Koushanfar, and Sani R Nassif. Ultra-low power current-based puf. In *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*, pages 2071–2074. IEEE, 2011.

[46] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*, volume 31. Springer Science & Business Media, 2008.

[47] James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. *Disruptive technologies: Advances that will transform life, business, and the global economy*, volume 180. McKinsey Global Institute San Francisco, CA, 2013.

[48] Cedric Marchand, Lilian Bossuet, Ugo Mureddu, Nathalie Bochard, Abdelkarim Cherkaoui, and Viktor Fischer. Implementation and characterization of a physical unclonable function for iot: a case study with the tero-puf. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2017.

[49] Thomas S Messerges, Ezzat A Dabbish, and Robert H Sloan. Examining smart-card security under the threat of power analysis attacks. *Computers, IEEE Transactions on*, 51(5):541–552, 2002.

[50] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan. Investigations of power analysis attacks on smartcards. *Smartcard*, 99:151–161, 1999.

[51] Câncio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine. Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level. *Microelectronics Journal*, 44(6):496–503, 2013.

[52] Câncio Monteiro, Yasuhiro Takahashi, and Toshikazu Sekine. Low-power secure s-box circuit using charge-sharing symmetric adiabatic logic for advanced encryption standard hardware design. *IET Circuits, Devices & Systems*, 9(5):362–369, 2015.

[53] Jagadeesh Subbaiah Moodera, Lisa R Kinder, Terrilyn M Wong, and R Meservey. Large magnetoresistance at room temperature in ferromagnetic thin film tunnel junctions. *Physical review letters*, 74(16):3273, 1995.

[54] Yong Moon and Deog-Kyoon Jeong. An efficient charge recovery logic circuit. *IEEE journal of solid-state circuits*, 31(4):514–522, 1996.

[55] Amir Moradi and Axel Poschmann. Lightweight cryptography and dpa countermeasures: A survey. In *Financial Cryptography and Data Security*, pages 68–79. Springer, 2010.

[56] Amir Moradi, Mohammad Taghi Manzuri Shalmani, and Mahmoud Salmasizadeh. Dual-rail transition logic: A logic style for counteracting power analysis attacks. *Computers & Electrical Engineering*, 35(2):359–369, 2009.

[57] Sumio Morioka and Akashi Satoh. An optimized s-box circuit architecture for low power aes design. In *Cryptographic Hardware and Embedded Systems-CHES 2002*, pages 172–186. Springer, 2002.

[58] Debdeep Mukhopadhyay. Pufs as promising tools for security in internet of things. *IEEE Design & Test*, 33(3):103–115, 2016.

[59] Adam Neale and Manoj Sachdev. A low energy sram-based physically unclonable function primitive in 28 nm cmos. In *Custom Integrated Circuits Conference (CICC), 2015 IEEE*, pages 1–4. IEEE, 2015.

[60] Thomas Popp and Stefan Mangard. Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 172–186. Springer, 2005.

[61] NIST FIPS Pub. 197: Advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197:441–0311, 2001.

[62] Fengbo Ren and Dejan Markovic. True energy-performance analysis of the mtj-based logic-in-memory architecture (1-bit full adder). *IEEE Transactions on Electron Devices*, 57(5):1023–1028, 2010.

[63] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of aes. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 413–427. Springer, 2010.

[64] Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents. In *International Conference on Smart Card Research and Advanced Applications*, pages 89–103. Springer, 2008.

[65] Carl A Schu, Daniel R Greeninger, and David L Thompson. Power dissipation reduction in medical devices using adiabatic logic, August 20 2002. US Patent 6,438,422.

[66] Sergei Petrovich Skorobogatov. *Semi-invasive attacks: a new approach to hardware security analysis*. PhD thesis, Citeseer, 2005.

[67] Stefano Stanzione, Daniele Puntin, and Giuseppe Iannaccone. Cmos silicon physical unclonable functions based on intrinsic process variability. *IEEE Journal of Solid-State Circuits*, 46(6):1456–1463, 2011.

[68] Ben G Streetman and Sanjay Banerjee. *Solid state electronic devices*, volume 4. Prentice Hall New Jersey, 2000.

[69] G Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual Design Automation Conference*, pages 9–14. ACM, 2007.

[70] Daisuke Suzuki, Minoru Saeki, and Tetsuya Ichikawa. Random switching logic: A new countermeasure against dpa and second-order dpa at the logic level. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 90(1):160–168, 2007.

[71] Sha Tao and Elena Dubrova. Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm cmos. *Electronics Letters*, 52(10):805–806, 2016.

[72] Philip Teichmann. *Adiabatic logic: future trend and system level perspective*, volume 34. Springer Science & Business Media, 2011.

[73] Himanshu Thapliyal, Fazel Sharifi, and S Dinesh Kumar. Energy-efficient design of hybrid mtj/cmos and mtj/nanoelectronics circuits. *IEEE Transactions on Magnetics*, 2018.

[74] Kris Tiri, Moonmoon Akmal, and Ingrid Verbauwhede. A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Solid-State Circuits Conference, 2002. ESSCIRC 2002. Proceedings of the 28th European*, pages 403–406. IEEE, 2002.

[75] Kris Tiri and Ingrid Verbauwhede. Charge recycling sense amplifier based logic: securing low power security ics against dpa. In *30th European Conference on Solid-State Circuits*, pages 179–182, 2004.

[76] Kris Tiri and Ingrid Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, page 10246. IEEE Computer Society, 2004.

[77] Wim Van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

[78] Anthony Van Herrewege. Lightweight puf-based key and random number generation. 2015.

[79] A Vetuli, S Di Pascoli, and LM Reyneri. Positive feedback in adiabatic logic. *Electronics Letters*, 32(20):1867–1868, 1996.

[80] Arunkumar Vijayakumar, Vinay C Patil, and Sandip Kundu. On improving reliability of sram-based physically unclonable functions. *Journal of Low Power Electronics and Applications*, 7(1):2, 2017.

[81] Tutu Wan, Yasha Karimi, Milutin Stanacevic, and Emre Salman. Energy efficient ac computing methodology for wirelessly powered iot devices. In *Circuits and Systems (ISCAS), 2017 IEEE International Symposium on*, pages 1–4. IEEE, 2017.

[82] Tutu Wan, Yasha Karimi, Milutin Stanaćević, and Emre Salman. Perspective papercan ac computing be an alternative for wirelessly powered iot devices? *IEEE Embedded Systems Letters*, 9(1):13–16, 2017.

[83] You WANG, Yue ZHANG, Jacques-Olivier Klein, Thibaut Devolder, Dafin Ravelosona, Claude Chappert, and Weisheng Zhao. Compact model for perpendicular magnetic anisotropy magnetic tunnel junction, Aug 2017.

[84] Marilyn Wolf. Ultralow power and the new era of not-so-vlsi. *IEEE Design & Test*, 33(4):109–113, 2016.

[85] Huapeng Wu. Bit-parallel finite field multiplier and squarer using polynomial basis. *IEEE Transactions on Computers*, 51(7):750–758, 2002.

[86] Kaiyuan Yang, Qing Dong, David Blaauw, and Dennis Sylvester. 14.2 a physically unclonable function with ber¡ 10- 8 for robust chip authentication using oscillator collapse in 40nm cmos. In *Solid-State Circuits Conference-(ISSCC), 2015 IEEE International*, pages 1–3. IEEE, 2015.

[87] Yibin Ye and Kaushik Roy. Qserl: Quasi-static energy recovery logic. *Solid-State Circuits, IEEE Journal of*, 36(2):239–248, 2001.

[88] Ramtin Zand, Arman Roohi, Soheil Salehi, and Ronald F DeMara. Scalable adaptive spintronic reconfigurable logic using area-matched mtj design. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 63(7):678–682, 2016.

[89] Yue Zhang, Weisheng Zhao, Yahya Lakys, Jacques-Olivier Klein, Joo-Von Kim, Dafiné Ravelosona, and Claude Chappert. Compact modeling of perpendicular-anisotropy cofeb/mgo magnetic tunnel junctions. *IEEE Transactions on Electron Devices*, 59(3):819–826, 2012.

[90] Weisheng Zhao, Mathieu Moreau, Erya Deng, Yue Zhang, Jean-Michel Portal, Jacques-Olivier Klein, Marc Bocquet, Hassen Aziza, Damien Deleruyelle, Christophe Muller, et al. Synchronous non-volatile logic gate design based on resistive switching memories. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(2):443–454, 2014.

# Vita

**Author name:** Dinesh Kumar Selvakumaran

**Education:**

**School name:** Indian Institute of Information Technology, Design and Manufacturing, Kancheepuram, India
**Degree:** Master of Design in Electronic System Design, May 2015

**School name:** Anna University, India
**Degree:** Bachelor of Engineering in Electronics and Communication Engineering, May 2013

**Experience:**

Graduate Research Assistant
Fall 2015- Fall 2018
University of Kentucky
Lexington, KY

**Professional Honors/Awards:**

1. Recipient of College of Engineering Deans award for outstanding PhD student, University of Kentucky, 2018.

2. Received United States Electric Corporation (USEC) Inc. Graduate Fellowship for the academic year 2017-2018.

3. Received "Best Paper Award" at 12th Annual Cyber and Information Security Research (CISR) conference 2017, for our paper titled, "UTB-SOI based adiabatic computing for low power and secure IoT devices".

4. Recipient of 2015 UPE/CS Award for Academic Excellence from the IEEE CS Upsilon Pi Epsilon Honor Society.

5. Received the Best project award for the work done on designing low-power Ternary Content Addressable Memory (TCAM) as master thesis in IIITDM, 2015

**Journal Publications:**

1. S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad, ”FinSAL: FinFET-Based Secure Adiabatic Logic for Energy-Efficient and DPA Resistant IoT Devices”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 37.1* (2018), pp. 110-122 .

2. S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad, ”EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card”, *IEEE Transactions on Emerging Topics in Computing* (2018) (accepted).

3. Himanshu Thapliyal, Fazel Sharifi, and S. Dinesh Kumar. ”Energy-Efficient Design of Hybrid MTJ/CMOS and MTJ/Nanoelectronics Circuits.” *IEEE Transactions on Magnetics, 54.7* (2018), p.3400908.

4. S Dinesh Kumar, Himanshu Thapliyal, Azhar Mohammad, and Kalyan S Perumalla, ”Design Exploration of Symmetric Pass Gate Adiabatic Logic for Energy-Efficient and Secure Hardware”, *Integration, the VLSI Journal,58* (2017), pp. 369-377.

5. Himanshu Thapliyal, Azhar Mohammad, S. Dinesh Kumar, and Fazel Sharifi. ”Energy-efficient magnetic 4-2 compressor.” *Microelectronics Journal 67* (2017), pp. 1-9.

6. S Dinesh Kumar, and Himanshu Thapliyal. ”Adiabatic Logic Based Energy Efficient and Reliable PUF for IoT devices”, *IEEE Transactions on Emerging Topics in Computing* (2018) (under review).

7. S Dinesh Kumar, and Himanshu Thapliyal. ”Exploration of Non-Volatile MTJ/CMOS Circuits for DPA Resistant Embedded Hardware”, *IEEE Transactions on Magnetics* (2018) (Under review).

8. S Dinesh Kumar, and Himanshu Thapliyal. ”Energy-Efficient MTJ/CMOS designs for DPA secure cryptographic hardware”, *ACM Transactions on Embedded Computing Systems* (2018) (To be submitted).

**Conference Publications:**

1. Zach Khaliefeh, S. Dinesh Kumar, and Himanshu Thapliyal. ”Hardware Trojan Detection in Implantable Medical Devices Using Adiabatic Computing.” *In proceedings of the IEEE International Conference on Rebooting Computing (ICRC),).* IEEE, 2018 (accepted).

2. S. Dinesh Kumar, Carson Labrado, Riasad Badhan, Himanshu Thapliyal, and Vijay Singh. ”Solar Cell Based Physically Unclonable Function for Cybersecurity in IoT Devices.” *In proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 697-702. IEEE, 2018.

3. Himanshu Thapliyal and S. Dinesh Kumar. ”Energy-recovery based hardware security primitives for low-power embedded devices.” *In proceedings of the IEEE International Conference on Consumer Electronics (ICCE),* pp. 1-6. IEEE, 2018.

4. S. Dinesh Kumar and Himanshu Thapliyal. ”Security Evaluation of MTJ/CMOS Circuits Against Power Analysis Attacks.” *In proceedings of the IEEE International Symposium on Nanoelectronic and Information Systems (iNIS),* pp. 117-122. IEEE, 2017.

5. Himanshu Thapliyal, T. S. S. Varun, and S. Dinesh Kumar. ”Low-Power and Secure Lightweight Cryptography Via TFET-Based Energy Recovery Circuits.” *In proceedings of the IEEE International Conference on Rebooting Computing (ICRC),* pp. 1-4. IEEE, 2017.

6. Himanshu Thapliyal, T. S. S. Varun, and S. Dinesh Kumar. ”Adiabatic Computing Based Low-Power and DPA-Resistant Lightweight Cryptography for IoT Devices.” *In proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI),* pp. 621-626. IEEE, 2017.

7. Himanshu Thapliyal, T. S. S. Varun, and S. Dinesh Kumar. ”UTB-SOI based adiabatic computing for low-power and secure IoT devices.” *In Proceedings of the 12th Annual Conference on Cyber and Information Security Research,* p. 16. ACM, 2017.

8. S. Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. ”FinSAL: A novel FinFET based Secure Adiabatic Logic for energy-efficient and DPA resistant IoT devices.” *In proceedings of the IEEE International Conference on Rebooting Computing (ICRC),* pp. 1-8. IEEE, 2016.

9. S. Dinesh Kumar , Himanshu Thapliyal, Azhar Mohammad, Vijay Singh, and Kalyan S. Perumalla. ”Energy-efficient and secure s-box circuit using symmetric pass gate adiabatic logic.” *In proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI),* pp. 308-313. IEEE, 2016.

10. S. Dinesh Kumar, and Himanshu Thapliyal. ”Qualpuf: A novel quasi-adiabatic logic based physical unclonable function.” *In Proceedings of the 11th Annual Cyber and Information Security Research Conference,* p. 24. ACM, 2016.