2022

# ENERGY-EFFICIENT AND SECURE HARDWARE USING ADIABATIC LOGIC AND NON-VOLATILE MTJ DEVICES

Zachary Kahleifeh
*University of Kentucky*, zachary.kahleifeh@uky.edu

Digital Object Identifier: https://doi.org/10.13023/etd.2022.263

## Recommended Citation

Kahleifeh, Zachary, "ENERGY-EFFICIENT AND SECURE HARDWARE USING ADIABATIC LOGIC AND NON-VOLATILE MTJ DEVICES" (2022). *Theses and Dissertations--Electrical and Computer Engineering*. 181.
https://uknowledge.uky.edu/ece_etds/181

Zachary Kahleifeh, Student

Dr. Himanshu Thapliyal, Major Professor

Dr. Dan Lau, Director of Graduate Studies

# ENERGY-EFFICIENT AND SECURE HARDWARE USING ADIABATIC LOGIC AND NON-VOLATILE MTJ 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
Zachary Kahleifeh
Lexington, Kentucky
Co-Director: Dr. Himanshu Thapliyal, Professor of
Co-Director: Dr. Mike Johnson, Professor of
Electrical and Computer Engineering
Lexington, Kentucky
2022

# ABSTRACT OF DISSERTATION

## ENERGY-EFFICIENT AND SECURE HARDWARE USING ADIABATIC LOGIC AND NON-VOLATILE MTJ DEVICES

Internet of Things (IoT) is a collection of devices that exchange data through a network to implement complex applications. IoT devices increase the quality of life of their user base which has a wide variety such as the medical field, consumer electronics, and the manufacturing sector. However, IoT devices have several challenges that need to be overcome namely, security and energy consumption. The threat vector that IoT devices face is growing and includes the following threats, the leakage of information through a side-channel attack known as the Correlation Power Analysis (CPA), authentication, piracy, etc. There are many countermeasures to CPA attacks, however, many of these countermeasures consume substantial energy which makes them non-ideal for IoT devices which are typically battery operated. In this thesis, we have explored the use of a novel, low-energy design technique known as adiabatic logic and an emerging memory technology known as Magnetic Tunnel Junctions (MTJ) to design ultra-low-energy and CPA resistant circuits for use in IoT devices.

Adiabatic logic is an ultra-low energy circuit design technique that utilizes power clocks to supply and recover charge from a circuit. Adiabatic logic is typically constructed using a 4-phase power clock however, the area and complexity of the power clock generator is a design limitation. Thus, the first contribution of this thesis is the conversion of an existing adiabatic logic family known as Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) into a functional and energy-efficient 2-phase implementation. 2-EE-SPFAL has less complex routing and less complex power clock design when compared to EE-SPFAL and is energy-efficient compared to standard CMOS. Furthermore, 2-EE-SPFAL has uniform power consumption regardless of data transition and thus is shown to be secure against power analysis attacks.

Adiabatic logic reduces the dynamic energy consumption of a circuit but as the technology node decreases through sub 45nm the leakage power of an integrated circuit becomes a limiting factor. To that end, the second contribution of this thesis is the design of a hybrid adiabatic and MTJ circuit architecture. One of the main advantages of MTJs is the near-zero leakage power they consume which is essential as technology nodes scale down. To create an ultra-low energy circuit, we combine the dynamic energy savings of adiabatic logic with the leakage power savings of MTJs to create Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML). We also show that EE-ACML is CPA resistant by implementing a lightweight cryptographic cipher utilizing EE-ACML and unsuccessfully stealing the encryption keys when performing a CPA attack.

Authentication, privacy, and secure key generation are important considerations when designing IoT devices. One security primitive that can aid in solving the aforementioned issues is the Physically Unclonable Function (PUF). The third contribution of this thesis is the design of a hybrid adiabatic/MTJ PUF. The proposed PUF saves energy by utilizing the energy recovery of adiabatic logic as well as the reduced leakage power with the implementation of the MTJs. The source of manufacturing variation within the proposed PUF is dominated by the variation of the MTJs.

The clock generator of an adiabatic circuit is an essential component of any adiabatic system. Adiabatic clock generators come in many forms based on the number of phases they produce. For example, a 2-phase clock generator can produce a 2-phase clock in the form of a sinusoidal waveform. Different adiabatic circuits are constructed using these different clock generators and are shown to be energy-efficient. However, there is a lack of comparison on clock generators in terms of both energy efficiency and security against power analysis attacks. Thus, we perform a comparative study on 2 and 4-phase clock generators to analyze the trade-offs between energy efficiency and security of adiabatic clock generators.

KEYWORDS: Adiabatic Logic, Magnetic Tunnel Junction, Physically Unclonable Functions, Cryptography, Side-Channel Attack, Correlation Power Analysis Attack.

Zachary Kahleifeh

July 13, 2022

ENERGY-EFFICIENT AND SECURE HARDWARE USING ADIABATIC LOGIC AND NON-VOLATILE MTJ DEVICES

By

Zachary Kahleifeh

Dr. Himanshu Thapliyal

(Co-Director of Dissertation)

Dr. Michael Johnson

(Co-Director of Dissertation)

Dr. Daniel Lau

(Director of Graduate Studies)

July 13, 2022

(Date)

Dedicated to my parents

Their unwavering support allowed me to start and end this story.

# ACKNOWLEDGEMENTS

My teachers have been the most important piece in my research journey, I express the deepest gratitude to my closest teacher, my adviser Dr. Himanshu Thapliyal. My growth as a researcher could not be possible without his patience, support, and guidance. I also thank my committee members, Dr. Mike Johnson, Dr. Hank Dietz, and Dr. D. Manivannan for their insightful suggestions to improve my research. I am grateful to Dr. Mike Johnson for serving as the Co-Chair of my committee as well as my fellowship coordinator.

I am very thankful to one of my early mentors Dinesh Kumar Selvakumaran who helped guide me at the beginning of my journey and set a foundation that allowed my research to succeed. The road to my Ph.D. was made easier by my lab mates Wu Yang, Carson Labrado, Edgard Munoz-Coreas, and Rajdeep Nath. I would like to give special thanks to my labmate Amit Degada for his constant willingness to discuss research, aid me in my research problems, and teach me his vast knowledge.

I would also like to thank the many friends I have for the love and support they provided throughout my dissertation journey. There is not enough room in this dissertation to name all of them and how they supported me but they should know they are a major reason for the completion of this work. I would especially like to thank my first friends, my brother, and my sister. Their support and challenges throughout my life have made me into the person I am today.

Lastly, it is impossible to put into words how grateful I am for my parents. My mother's love and support has given me the strength and guidance to overcome any challenge. My mother taught me that any challenge can be overcome with enough patience. I am also thankful for my father teaching me the importance of handwork, leadership, and the pursuit of knowledge.

This work was supported by the Graduate Assistance in Areas of National Need Fellowship and National Science Foundation CAREER Award No. 1845448.

# Table of Contents

List of Figures

List of Tables

# Chapter 1

# Introduction

The Internet of Things (IoT) can be loosely defined as a connection of devices that share information through a network. This can include consumer electronics such as the Nest by Google which consists of various devices (thermostats, cameras, sensors, etc.) communicating with each other to improve the ease of life of the user. IoT can also find itself improving the productivity of the manufacturing sector [13] through the use of sensors sharing information to enable intelligent applications. Home consumer electronics and the manufacturing sector are only two of the many applications of IoT devices, in the modern technological world, many areas are including IoT devices such as those seen in Figure 1.1. The number of IoT devices continues to increase year after year as Cisco predicts the number of IoT devices to reach 29.3 billion in 2023, compared to 18.4 billion in 2018 [14]. Furthermore, the economic impact of IoT devices is substantial, Frontier economics estimates IoT devices will increase the US GDP by $2.23 trillion between 2018 and 2032 [15]. These statistics show the importance and growth of IoT devices in the modern technological world.

## 1.1 The Challenges IoT Devices Face

IoT devices store and transmit information over a shared network to perform a complex application. There are numerous areas where IoT can be applied and each area contains a specific set of requirements. Two requirements that are common among many areas of IoT devices are the energy consumption and security of an IoT device. Both of these requirements are two challenges that must be overcome if IoT is to continue growing.

### 1.1.1 Energy Consumption

The energy consumption of integrated circuits (ICs) that power IoT devices continues to grow with each new generation. This would not be a major issue in desktop or laptop computers as they are either directly connected to power or the area is large enough to include a sufficient battery. Unlike the aforementioned devices, IoT devices typically have reduced area, are portable, and have limited human interaction. Thus, batteries are typically used to power these devices for ample amounts of time. The area limitations of IoT devices limit the size of the battery and thus become a major constraint. The major sources of power consumption within the ICs that drive IoT

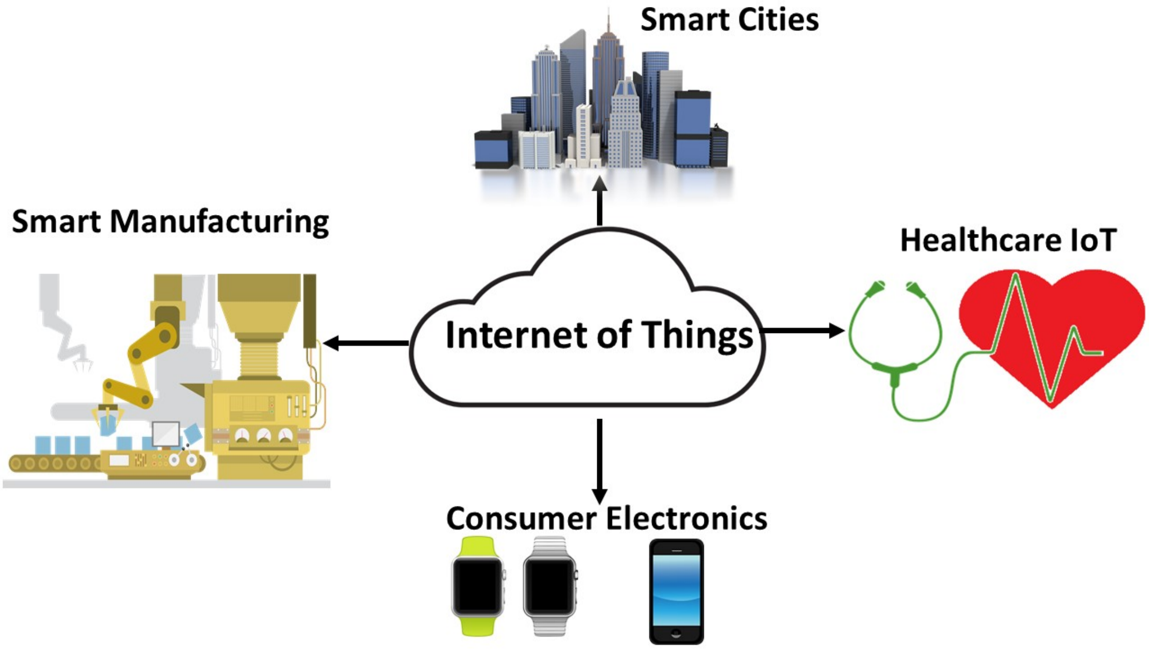


Figure 1.1: Various applications of IoT devices.

devices include dynamic power consumption and static power consumption. Figure 1.2 shows the static and dynamic power trends as technology node decreases [1]. As the technology node decreases, both dynamic and stand-by power increases thus it is important to design energy-efficient IoT designs for future generations.

### Design Techniques and Emerging Devices to Reduce Dynamic Energy Consumption

To reduce the dynamic energy consumption of IoT devices, various logic design techniques can be implemented. Such design techniques include dynamic voltage and frequency scaling (DVFS). DVFS involves scaling the supply voltage and frequency when peak performance is not necessary to reduce the power consumption. DVFS is limited by the threshold voltage of a transistor and has been shown to have diminishing returns at a certain point [16]. Adiabatic logic is another design technique used to reduce the dynamic power consumption of a circuit [17]. Through the use of time ramp voltage power clocks, adiabatic logic recovers energy stored in load capacitors to be reused again in the next cycle thus reducing energy consumption. Adiabatic power clocks utilize capacitors and inductors to generate the clock signal while also using these devices to store the recovered energy [18]. Energy is stored in these devices through an electric charge in the capacitors and magnetic energy in the inductor.

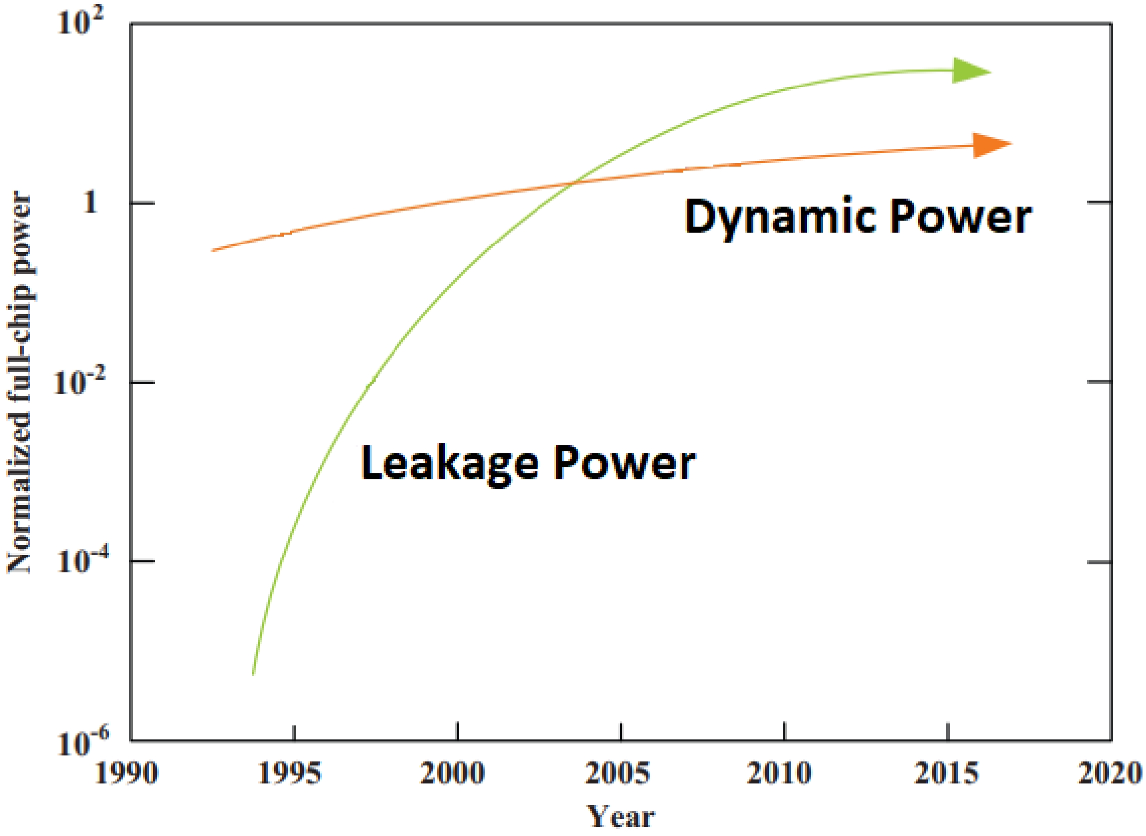


Figure 1.2: Leakage and dynamic power trends [1].

### Design Techniques and Emerging Devices to Reduce Static Energy Consumption

Static energy consumption has become a major issue as the technology node has scaled-down. One design technique that has been developed and implemented is multi-threshold transistor designs. Multi-threshold designs are circuits that use different transistors with different threshold voltages depending on if they are in critical paths. Higher threshold voltage transistors have lower static power while at the same time they increase the delay. Thus, critical paths that require low delay use low threshold voltage transistors while less critical paths use high threshold transistors to reduce leakage power. Emerging devices and technologies have come to the forefront as potential solutions to energy constraint issues. As the technology node decreases, the standard MOSFET device was not able to keep up with power and delay constraints. Thus, industries adopted FinFET-based devices to better control the gate current and thus reduce leakage power and delay. Even with the introduction of FinFETs into modern ICs, power consumption continues to increase and thus more emerging devices should be investigated. Emerging memory technologies have been explored to introduce a Logic-in-Memory (LiM) architecture to further reduce power consumption. There are many design choices for the non-volatile memory that is implemented in LiM structures such as Magnetic Tunnel Junctions (MTJ)[19], Phase Change Memory (PCM)[20], and MEMristors[21]. Among these memory technologies, MTJs are considered a promising choice because they offer the following advantages: near-zero leakage power, high integration density, and easy compatibility with CMOS [12, 22, 23]. Hybrid MTJ/CMOS LiM circuits have been shown to reduce power and thus are promising implementation choices in power-constrained IoT devices. Further, MTJs have been implemented into commercial memories by companies such as Everspin which shows their promise in replacing the standard technologies [24].

### 1.1.2 Security

The threat vectors of IoT devices continue to grow thus new defenses against attacks must be developed. IoT devices can be used to store and transmit sensitive data such as the data used within the healthcare IoT [25]. Thus, IoT devices are targets for attack. Within an area and energy-constrained IoT device, security is not prioritized which leads to weaknesses in the device. When security modules are added to IoT devices they are typically added at the software level using techniques that are also commonly employed in other computing devices such as desktop computers and servers. However, this defense does not cover all possible attack mechanisms such as those on the hardware of the device.

### Side-Channel Attacks on IoT devices

The main defense within IoT devices to secure stored information is through the use of encryption. Encryption algorithms use secret keys to prevent data from being stolen. If these keys were to be recovered, the IoT device can no longer be considered

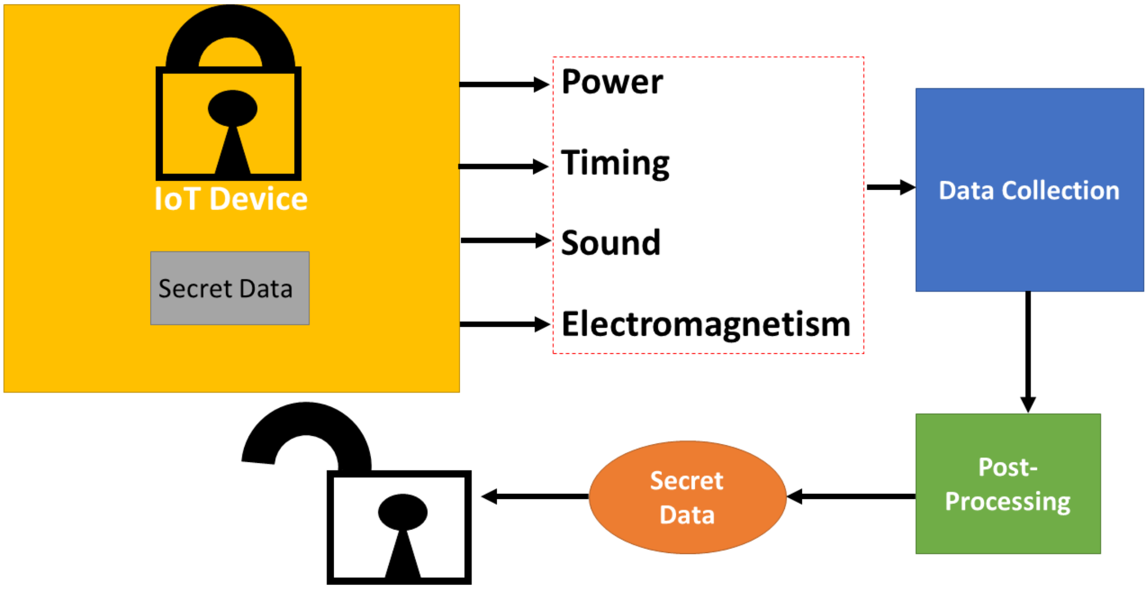


Figure 1.3: Generic process of a side-channel attack.

secure. One type of attack that IoT devices can face is a side-channel attack. A side-channel attack is a non-invasive attack that looks to steal information through a device's side channels which can include power consumption, timing, etc. A side-channel attack can be used to steal the encryption keys that keep IoT devices secure. Ronen et al. have shown that side-channel attacks can be used on IoT devices as they performed one on a Phillips Hue smart lamp and were able to take control of it [26]. Further, side-channel attacks played a major role in the implementation of Spectre and Meltdown attacks which allow for an attacker to gain access to restricted memory areas [27, 28].

Among the side-channel attacks, power analysis attacks are very dangerous to encryption algorithms as they can be used against both synchronous and asynchronous encryption algorithms. The Simple Power Analysis attack (SPA) was originally developed to break encryption circuits by visually inspecting the power consumption of a circuit. However, SPA attacks could be prevented through the use of masking and hiding techniques. Using the ideas behind SPA and timing-based side-channel attacks, Paul Kocher developed the Differential Power Analysis attack (DPA) which instead of using visual inspection used statistical analysis and error correction to recover the key [29]. Improvements have been made to the DPA attack ultimately leading to the Correlation Power Analysis attack (CPA) which can recover encryption keys more quickly than both the SPA and DPA.

### Key generation and Authentication

Key generation for the encryption circuits that defend IoT devices is an essential part of securing IoT devices. Keys are commonly stored in non-volatile memory which is

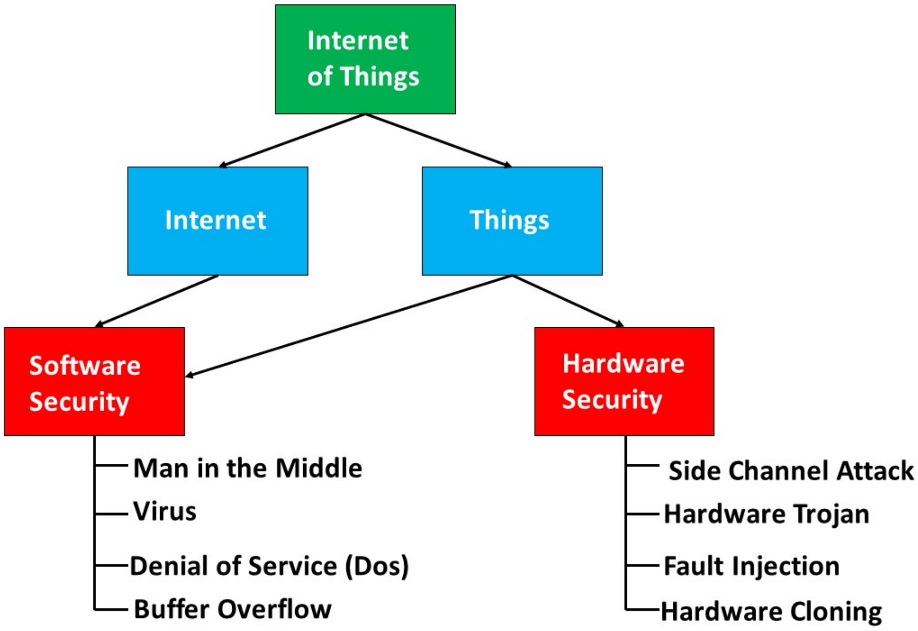


Figure 1.4: Various attacks that IoT devices face from both the software and hardware level [2].

prone to physical attacks and can be costly on already area and power-constrained IoT devices. Further, the defenses against physical attacks such as tamper-resistant packaging add to the cost and area of the device [30]. Encryption keys are an essential part of authenticating a device. Many of the attacks that IoT devices face are a result of improper authentication of a device or cloning of a device. These attacks can be widespread and detrimental as Gartner reports that 20% of companies have experienced at least one IoT attack in the past three years [31].

## 1.2 Motivation

IoT is an essential component in improving the quality of life of the common user. Further, IoT devices can be implemented by corporations to improve the efficiency of their manufacturing. As useful IoT devices may be, they also have limitations such as the security and energy consumption of the device. There are numerous survey papers discussing the various security issues related to IoT devices [32–35]. A common theme among the surveys is that there are a large number of unique threats and challenges that IoT devices face because of the limited computation power and limited battery supply. Figure 1.4 shows various attacks that IoT devices face at both the software and hardware level.

Of the attacks mentioned, side-channel attacks are one of the more promising attacks for adversaries trying to access restricted information. While a device is operating (such as encrypting data) it releases side-channel information. Side-channel information can come in many forms such as power [29], acoustics[36], timing[37], electromagnetism[38], etc.

Table 1.1: Various circuits and their trade-offs.

| Parameter | CMOS | WDDL | SABL | EE-SPFAL |
|---|---|---|---|---|
| Energy | Medium | High | High | Low |
| CPA Resistant? | No | Yes | Yes | Yes |
| Area | Low | High | High | High |

Side-channel attacks have already been demonstrated on real-world applications such as Ronen et al. using a power-based side-channel attack to steal the key of a Phillips Hue smart lamp [26]. The power analysis attack performed on the smart lamp allowed researchers to gain access to a master key which in turn allowed them to change the firmware of the device. A power analysis attack was also performed on the ATMEGA328P microcontroller (a common microcontroller in IoT devices) showcasing the ability to steal keys from IoT processors [39]. It can be seen that power analysis-based side-channel attacks are a major threat to IoT devices. Among the power analysis attacks, the Correlation Power Analysis attack (CPA) is one of the more dangerous types of attack. Various techniques have been presented to defend against power analysis attacks. Such defenses can be split into two categories, hiding and masking-based defense [40]. Hiding involves reducing the correlation between power consumption and input transition such as making the power consumption uniform throughout. Hiding can be implemented on the circuit level through techniques such as Sense Amplifier Based Logic (SABL)[41] and Wave Dynamic Differential Logic (WDDL)[42]. These proposed circuit design techniques consume substantial power (even greater than CMOS equivalent designs) and thus are not suitable for implementation in battery-constrained IoT devices. Another hiding-based circuit level design is adiabatic logic, adiabatic logic is a low energy design technique that can be designed such that power consumption is uniform throughout.

Table 1.1 lists the trade-offs of various circuit design techniques. CMOS is the standard design choice for modern integrated circuits. It has a high switching speed and low area but the power consumption is dependent on data transitions. WDDL and SABL are two circuit designs that produce uniform power consumption at the cost of higher power consumption. EE-SPFAL is an adiabatic CPA-resistant circuit that has low energy consumption at the cost of using more transistors. The uniform power consumption and reduced energy of adiabatic circuits have motivated more research into the use of adiabatic logic for CPA-resistant circuits.

Along with the security of an IoT device, energy constraints have also been a motivating interest for researchers. New technologies have been developed to reduce the energy consumption of an integrated circuit (IC). One technology that has found itself being implemented in modern ICs is the FinFET. The short channel effects that occur in MOSFET-based devices were difficult to control as the technology size scaled down below 20nm [43]. The introduction of FinFETs allowed for more channel control of the device and thus reduced leakage power. However, power consumption continued to increase as technology nodes scale down and more transistors are added to the chip while following Moore's law. Thus more technologies were researched

Table 1.2: Summary of standard and emerging memory technologies.[8–10]

| | **SRAM** | **DRAM** | **Flash (NAND)** | **RRAM** | **PCM** | **STT-MRAM** |
|---|---|---|---|---|---|---|
| **Non-volatile?** | No | No | Yes | Yes | Yes | Yes |
| **Write Latency (ns)** | <2 | 50 | $10^6$ | 50 | $10^2$ | 10 |
| **Read Latency (ns)** | <2 | 30 | $10^3$ | <20 | 2 | <10 |
| **Ewrite/ Bit** | ∼1fJ | ∼10fJ | ∼10fJ | ∼0.1pJ | ∼10pJ | ∼0.1pJ |
| **Endurance** | $10^{16}$ | $10^{16}$ | $10^5$ | $10^6$ | $10^{10}$ | $10^{15}$ |
| **Cell Size ($F^2$)** | 50-120 | 6-10 | 5 | 6-10 | 4-19 | 6-20 |

to further reduce the energy consumption of an IC. Such technologies can be found in the form of emerging memory technologies such as Magnetic Tunnel Junctions (MTJ)[19], Phase Change Memory (PCM)[20], and MEMristors[21]. These emerging memory devices look to replace the typical IC-based memory elements such as SRAM, DRAM, and Flash memory. Table 1.2 shows the various advantages and disadvantages of emerging memory technologies when compared with standard IC memories.

From Table 1.2 we can see that MTJs are a promising replacement for various levels of the memory hierarchy. MTJs have the property of being non-volatile which both SRAM and DRAM lack. Further, the write and read latency of MTJs generally range between SRAM and DRAM latency while being much lower than flash latency. The endurance of the MTJs is also on par with the endurance of SRAM and DRAM and much higher than flash endurance. The drawbacks of the MTJs include high write current, the large cell size, and the reliability of the MTJs. Research is currently being done to reduce the write energy and increase the reliability of the MTJs through different write methods such as Spin-Orbit Torque [44].

Hybrid CMOS/MTJ circuits have been explored to design low-energy circuits. MTJs having near-zero leakage power make them an ideal choice to replace the current memory technologies in IoT devices. However, the FET-based portion of the hybrid circuits still consumes substantial dynamic power. To this end, we look to use adiabatic logic to design an energy-efficient hybrid adiabatic/MTJ architecture. Further, when the data in MTJs is switched it becomes susceptible to power analysis attacks. This motivated us to design a secure adiabatic/MTJ circuit that does not switch data and thus is secure against power analysis attacks.

Another aspect of building secure integrated circuits is the key generation for encryption circuits which also relates to authentication and privacy. One attack that IoT devices can face is the cloning attack. This attack involves an unauthorized device gaining access to the network by acting like a correct device [45]. A potential solution to these types of attacks and secure key generation is using a device known as a Physically Unclonable Function (PUF). PUFs can give devices a unique digital fingerprint and can thus authenticate a device to prevent cloning attacks. There are many types of PUFs that have been researched and developed such as arbiter PUF [46], Ring Oscillator PUF [47], and the SRAM PUF [30, 48, 49]. However, many of these proposed PUFs have issues when implementing them in IoT devices such as low reliability and high energy consumption. PUFs with low reliability require extra circuitry to operate such as Fuzzy Extractors and Error-Correcting Codes (ECC). This extra circuity increases the energy consumption and increases the area of ICs.

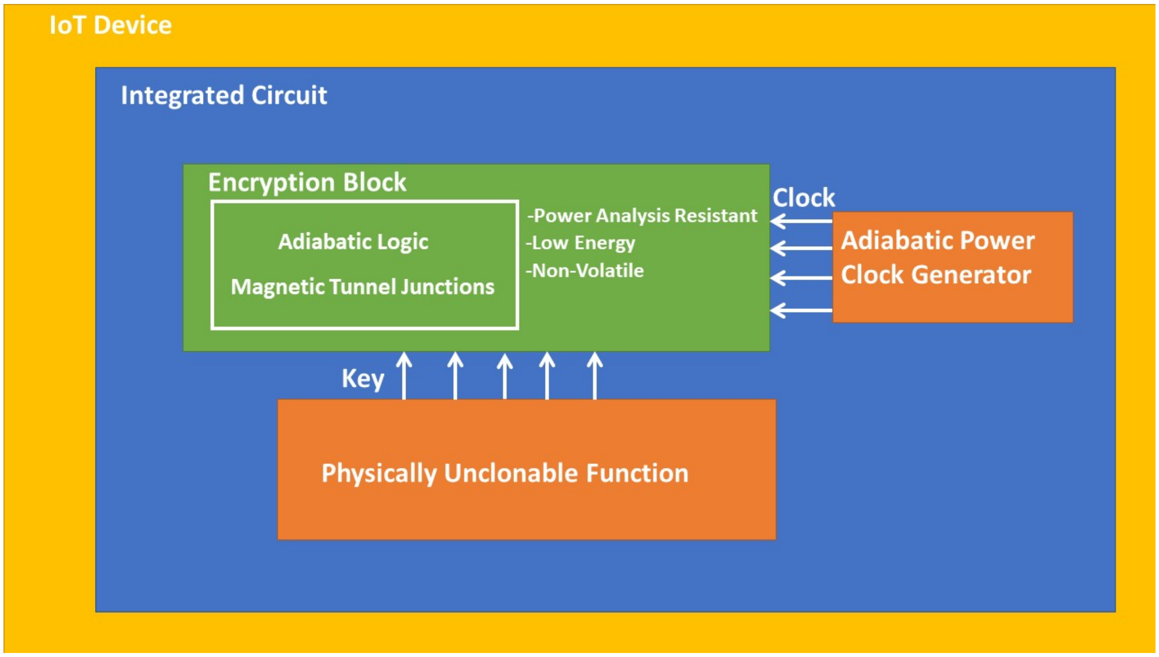

IoT Device
Integrated Circuit
Encryption Block
Adiabatic Logic
Magnetic Tunnel Junctions
-Power Analysis Resistant
-Low Energy
-Non-Volatile
Clock
Adiabatic Power Clock Generator
Key
Physically Unclonable Function

Figure 1.5: Low energy, power analysis resistant encryption block based on adiabatic logic and Magnetic Tunnel Junctions

Thus, we look to develop a low-energy and reliable PUF circuit using both adiabatic logic and MTJs.

The clock generation and distribution is an essential aspect of adiabatic circuits. The adiabatic clock generator can consume substantial power when generating the clock. Thus, it is important to ensure that the clock generator does not counteract the overall energy savings of an adiabatic circuit. Further, the adiabatic clock generator contains the storage elements for the energy recovered from an adiabatic circuit thus they should be able to efficiently recycle energy. As adiabatic clock generators are the driving force of adiabatic circuits, they can also affect the security against power analysis attacks. When a power analysis attack is performed, the clock generator should result in no information leakage. Energy and security are important issues to the many different types of adiabatic clocks. Currently, there is no comparison between adiabatic clock generators on both the energy efficiency and security of power analysis-resistant adiabatic circuits. Thus, a comparative study needs to be performed to determine the trade-offs between the two main types of adiabatic clock generators.

## 1.3 Problem Statements and Contribution

This section presents the contributions that are made in this thesis to design low-energy and secure IoT devices based on emerging technologies and design techniques. The novel work presented in this thesis is summarized in Figure 1.5.

### 1.3.1 Two-Phase Energy-Efficient Secure Positive Feedback Logic (2-EE-SPFAL)

**Problem Statement 1:**

Energy-Efficient Secure Positive Feedback Logic (EE-SPFAL) is a dual-rail adiabatic logic circuit. The original implementation of EE-SPFAL operates using a four-phase trapezoidal clocking scheme. To remain CPA resistant, EE-SPFAL requires four separate clocks and four separate discharge signals. This can lead to a large amount of interconnects which can result in a large area consumption on post-layout chip designs. Further, a four-phase clocking design can be more complex than its two-phase counterpart. In this portion of the thesis, we convert the existing EE-SPFAL into a two-phase version that remains energy-efficient and CPA resistant.

The key contributions of this work are as follows:

**Key Contribution 1:**

- This work presents 2-EE-SPFAL, a novel two-phase sinusoidal clocking implementation of Energy-Efficient Secure Positive Feedback Logic (EE-SPFAL).
- The case study implementation using 2-EE-SPFAL saves between 76.5% and 21.3% energy consumption at frequencies between 100kHz and 25 MHz when compared with its CMOS counterpart.
- The area of the design is reduced when compared with EE-SPFAL as the number of clock and discharge signals are reduced.
- We demonstrate that 2-EE-SPFAL is secure against power analysis attacks by performing a CPA attack on an encryption circuit implemented with 2-EE-SPFAL. The key could not be recovered when using 2-EE-SPFAL, however, when using CMOS the key could be stolen.

### 1.3.2 Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML)

**Problem Statement 2:**

CMOS-based circuits consume substantial dynamic energy consumption and the FETs that make up the circuits consume large amounts of leakage power. Adiabatic logic and MTJs are two emerging technologies that can be used to reduce dynamic and leakage power consumption. However, the switching of MTJs consumes substantial energy consumption and can be targeted with CPA attacks. Thus, in this part of the research Energy-Efficient Adiabatic MTJ/CMOS Logic (EE-ACML) is proposed to design energy-efficient and secure circuits. Using the proposed circuit we design secure encryption circuits that do not switch the MTJs thus saving energy and preventing CPA attacks.

The key contributions of this work are as follows:

**Key Contribution 2:**

- This work presents Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML), a novel hybrid adiabatic MTJ circuit.
- This work combines 2-EE-SPFAL and EE-ACML to construct a low energy and secure implementation of the PRESENT encryption standard.
- The proposed implementation of PRESENT reduces energy consumption between 66.99% and 86.58% at frequencies between 12.5MHz and 100MHz when compared with a CMOS/MTJ design proposed in the literature.
- We present the effect of varying the inductance and capacitance of the two-phase clock generator on both the energy consumption of a circuit and on the security of the circuit.
- We demonstrate the resilience of the circuit against power analysis attacks by unsuccessfully stealing a secret key while performing a CPA attack.

### 1.3.3 Hybrid Adiabatic/MTJ Physically Unclonable Function

**Problem Statement 3:**

Key generation, authentication, and privacy are essential components of a secure IoT device. The PUF is a security primitive that can be used to solve the previously mentioned issues. In this problem, we design a hybrid adiabatic/MTJ PUF. The adiabatic/MTJ PUF is a low-energy PUF design that utilizes process variation of the MTJs to generate a secure response output.

**Key Contribution 3:**

The key contributions of this work are as follows:

- We developed a novel Physically Unclonable Function using adiabatic logic and Magnetic Tunnel Junctions. The proposed PUF can generate two response bits per cell depending on the orientation of the MTJs.
- Monte Carlo simulations of the proposed PUF demonstrate strong security results using common metrics known as Uniqueness, Uniformity, and Reliability. Further, our proposed PUF is low energy as the PUF uses 5.2 and 5.1 fJ/Cycle depending on the orientation of the MTJ.
- The uniqueness of a PUF tells us how different the PUF is from other PUFs, the ideal value of uniqueness is 50%. Our proposed PUF results in uniqueness values of 49.98% and 49.99% depending on the orientation of the MTJs.
- The uniformity of a PUF tells us how many 0's and 1's make up the response bit, the ideal uniformity value is 50%. Our proposed PUF results in uniformity values of 50.18% and 50.17% depending on the orientation of the MTJs.

- The reliability of a PUF tells us how the response changes when environmental conditions change such as supply voltage and temperature. The ideal value of reliability is 100% which represents no change in the response from the ideal conditions to the non-ideal conditions. Our proposed PUF has a reliability of 97.07% and 96.97%.
- We have implemented our PUF as a key generator that produces a 64-bit key. This key is then used to generate the encrypted output using PRESENT encryption based on both 2-EE-SPFAL and EE-ACML. This circuit demonstrates a secure and low-energy implementation of encryption algorithms.

### 1.3.4 Comparison of two-phase and four-phase adiabatic clock generators for low-energy IoT devices

**Problem Statement 4:**

The adiabatic clock generator is an important component of any adiabatic circuit. The most common adiabatic circuits are based on two and four-phase clocking schemes. Thus, in this problem, we look to compare both the energy consumption and security of the two-phase and four-phase implementations of adiabatic circuits.

The key contributions of this work are as follows:

**Key Contribution 4:**

- We have constructed adiabatic circuits using both two and four-phase clocking schemes to ensure correct functionality.
- We have performed a literature study that shows two and four-phase clock generators are resilient against power analysis attacks.
- We have compared two and four-phase adiabatic clocks to determine which is more energy-efficient. We have determined that two-phase clocking schemes are more energy-efficient when compared with four-phase clock generators. We have found that two-phase clock generators consume less energy than four-phase clock generators at frequencies between 12.5 MHz and 200 MHz. We have also varied the load and temperature of the test circuits to determine the effects on clock generators.
- We have compared the two and four-phase clock generator security characteristics and determined that the four-phase clock generator has better security against power analysis attacks. The four-phase clock generator has NED and NSD values of 0.014 and 0.007, respectively. The two-phase clock generator has NED and NSD values of 0.110 and 0.060, respectively.

## 1.4 Thesis Organization

The organization of the thesis is as follows. Chapter 2 presents the background information necessary to understand the research advancements made in this thesis.

Chapter 2 covers background information on adiabatic logic, adiabatic power clock generators, Correlation Power Analysis Attacks, Magnetic Tunnel Junctions (MTJ), CMOS/MTJ hybrid circuits, and finally Physically Unclonable Functions. Chapter 3 presents the proposed 2-Energy-Efficient Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL) which is the two-phase implementation of EE-SPFAL. In Chapter 4, we present our proposed hybrid adiabatic/MTJ architecture known as Energy-Efficient Adiabatic CMOS/MTJ Logic. In Chapter 5, we present our proposed Physically Unclonable Function based on both adiabatic logic and MTJs. In Chapter 6, we present our comparison of adiabatic clock generators to determine the tradeoffs each circuit has. Chapter 7 concludes the dissertation report.

The work presented Chapter 3 is published in IEEE Consumer Electronics Magazine [7] and IEEE World Forum on Internet of Things [50]. Chapter 4 is published in IEEE Computer Society Annual Symposium on VLSI [51] and MDPI Sensors [52]. The work presented in Chapter 5 is currently under review in IEEE transactions on Consumer Electronics.

# Chapter 2

# Background and Related Work

The purpose of this chapter is to cover the background information on various security areas to understand the importance of securing IoT devices. This chapter goes into detail on the steps to perform a Correlation Power Analysis Attack (CPA) and Physically Unclonable Functions. Further, this chapter will discuss the background information necessary to understand adiabatic logic and adiabatic logic clock generators. This chapter also presents information on Magnetic Tunnel Junctions (MTJs) and hybrid CMOS/MTJ circuits.

## 2.1 Adiabatic Logic

Adiabatic logic is an emerging design technique for designing low-energy circuits [17]. Adiabatic logic utilizes a varying voltage source as opposed to a constant voltage source used in CMOS circuits. The varying voltage source allows for energy to be recovered back into the adiabatic clock when there is a potential difference between output and clock. The varying voltage source can take many forms such as a sinusoidal, triangular, or trapezoidal waveform. Figure 2.1 illustrates the structure of an adiabatic circuit and its charging/discharging of the load capacitors. The energy efficiency of adiabatic logic can be exemplified by analyzing the RC network of a FET-based circuit as seen in Figure 2.2. To calculate the energy dissipated in an adiabatic circuit we can use the following calculations.

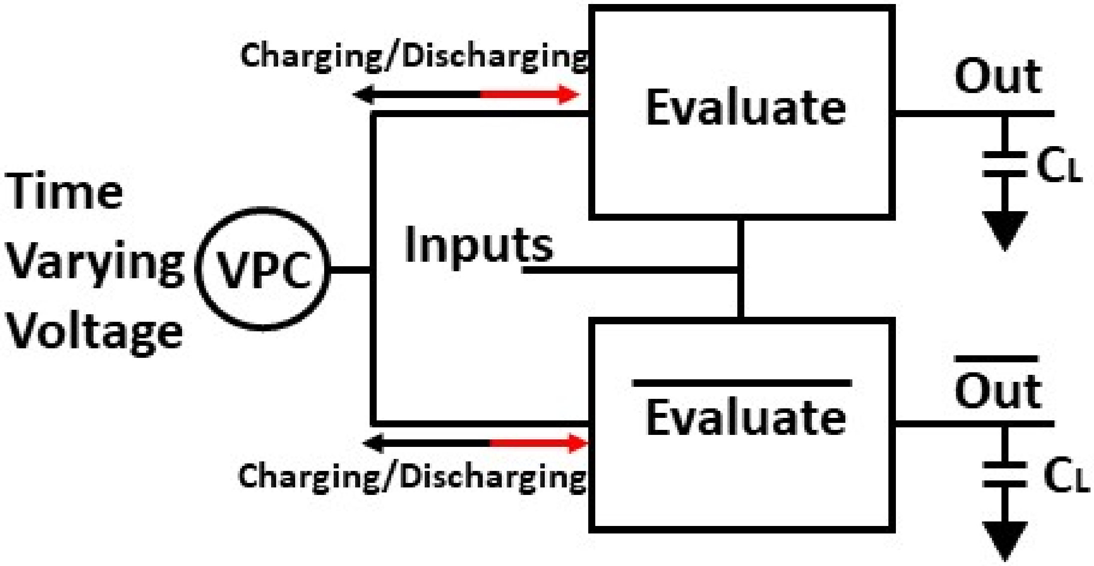


Figure 2.1: General structure of adiabatic logic circuits.

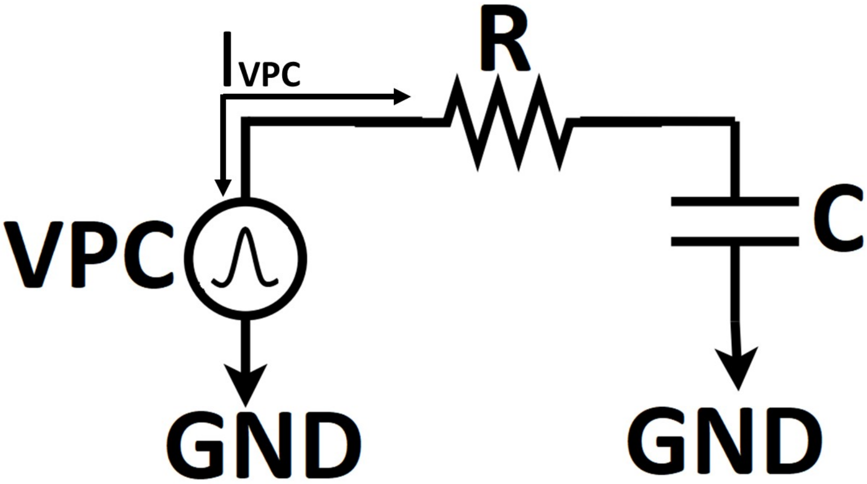


Figure 2.2: RC network of adiabatic FET-Based Circuit.

$$Ri(t) + \frac{1}{C}\int i(t)dt = \frac{V_{dd}}{T}t \tag{2.1}$$

We can apply the Laplace transform on equation 2.1 to arrive at the following equation.

$$\begin{aligned} RI(s) + \frac{1}{C_s}I(s) &= \frac{V_{dd}}{s^2T} \\ I(s) = \frac{C_sV_{dd}}{(RC+1)s^2\tau} &= \frac{V_{dd}C}{T}(\frac{1}{s} - \frac{1}{s+\frac{1}{RC}}) \end{aligned} \tag{2.2}$$

After applying the inverse Laplace transform on equation 2.2 we arrive at

$$i(t) = \frac{V_{dd}C}{T}(1 - e^{-\frac{1}{RC}t}) \tag{2.3}$$

After finding the current we can determine the power of an adiabatic circuit using the following equation.

$$p(t) = i^2R = R\frac{V_{dd}^2C^2}{T^2}(1 - 2e^{-\frac{1}{RC}t} + e^{-\frac{2}{RC}t}) \tag{2.4}$$

To calculate the energy for a period ranging from 0 to T we integrate the previous power equation from 0 to T.

$$\begin{aligned} E &= \int_0^T p(t)dt + E(0) \\ &= R\frac{V_{dd}^2C^2}{T^2}[t - 2RCe^{-\frac{2}{RC}t} - \frac{RC}{2}e^{-\frac{1}{RC}t}]_0^T \\ &= R\frac{V_{dd}^2C^2}{T^2}(2RCe^{-\frac{1}{RC}t} - \frac{RC}{2}e^{-\frac{2}{RC}t} - \frac{3RC}{2} + T) \end{aligned} \tag{2.5}$$

Using the assumption that T is >> greater than RC we can estimate the energy consumption to be

$$E_{diss,adiabatic} = \frac{RC}{T}CV_{dd}^2 \tag{2.6}$$

Where $T$ is the period of the adiabatic clock, $C$ is the capacitive load of the output, and $V_{dd}$ is the max voltage of the adiabatic clock. By equation 2.6, if the clock period T is greater than RC then the energy consumption will be lower than a standard CMOS circuit.

### 2.1.1 Adiabatic Power Clock Generators

The adiabatic clock generator is an essential component of an adiabatic circuit. Adiabatic clocks can come in many forms and can be differentiated by their number of phases and shapes. For example, an adiabatic clock can produce a two-phase output with a sinusoidal shape or a four-phase output with a trapezoidal shape. In this dissertation, we will focus on the two-phase and four-phase adiabatic clock generators. Adiabatic clock generators can further be classified into synchronous and asynchronous clock generators. Asynchronous clock generators are self-oscillating without the use of external signals. Asynchronous clock generators have many issues such as their frequencies being sensitive to variations in capacitors, increased power consumption, and are only used to generate two-phase signals. On the other hand, synchronous clock generators oscillate with the help of external signals to produce the desired frequency.

The basis for adiabatic clock generators is inductors and capacitors forming an RLC-based circuit. The clock generator in Figure 2.3 shows a two-phase sinusoidal clock generator [3]. The clock generator consists of a dual-rail LC oscillator and cross-coupled pairs of NMOS and PMOS transistors. The clock generator in Figure 2.3 utilizes the capacitance and resistance from the load circuit (labeled as $C_L$ and $R_L$) to generate the resistance and capacitance necessary to generate the RLC oscillator. Additional capacitance is used to balance the capacitance (labeled as $C_B$) at each output to improve efficiency.

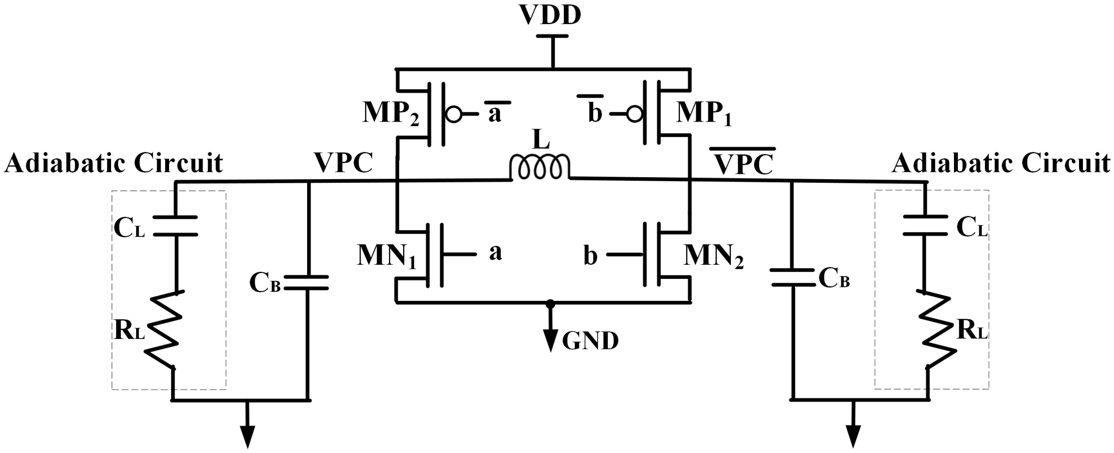


Figure 2.3: Structure of two-phase adiabatic clock generator. [3]

The frequency of the two-phase adiabatic clock generator is determined by setting the control signals properly and by following equation 2.7. The control signals used for the two-phase clock are shown in figure 2.4.

$$f = \frac{1}{2\pi\sqrt{LC}} \tag{2.7}$$

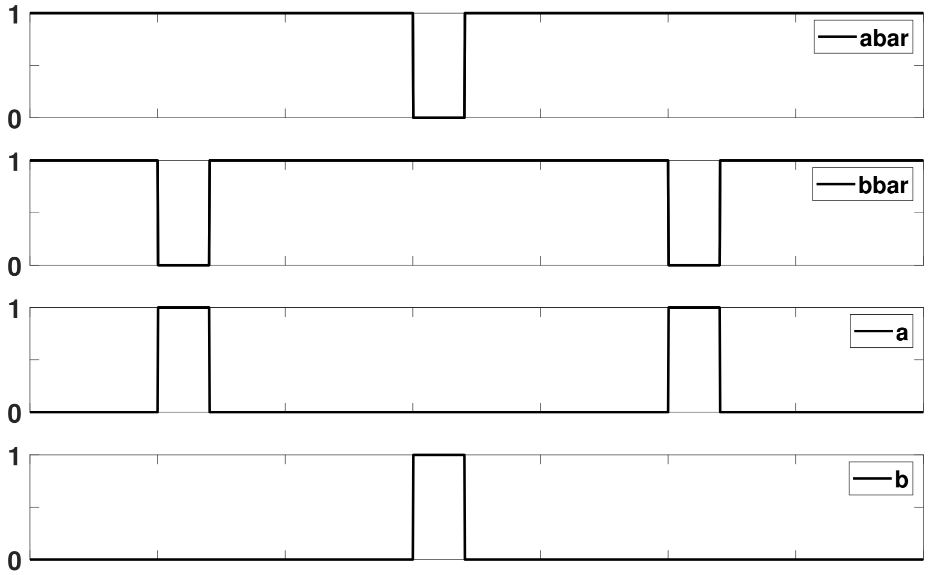


Figure 2.4: Control signals necessary to create a synchronous two-phase clock generator.

The four-phase adiabatic clock generator can be constructed in a similar manner. The four-phase clock generator is shown in Figure 2.5. The structure is similar to the two-phase clock generator in that an RLC-based circuit is used to generate the ramping effect needed for adiabatic circuits. The difference in structure comes from the clock rail driver. In a four-phase clock generator, the active driving network consists of a transmission gate and a pair of PMOS and NMOS transistors for each clock signal. The driver circuit is controlled by various external signals to ensure synchronous functionality.

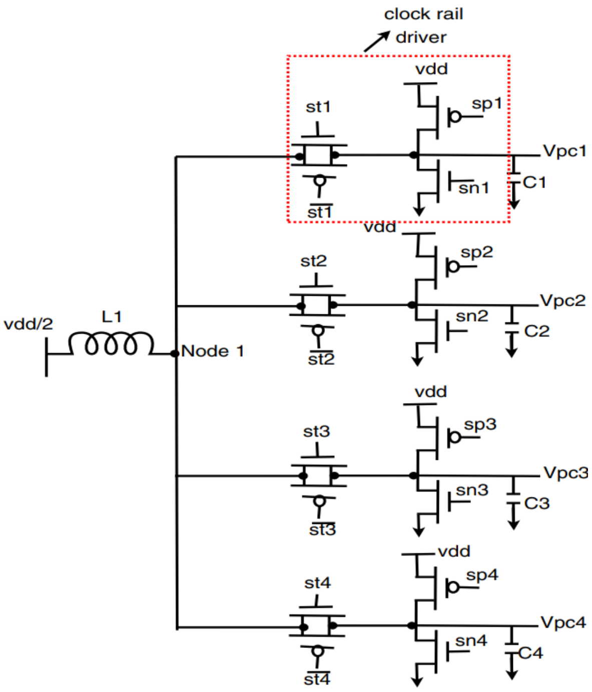


Figure 2.5: Structure of four-phase adiabatic clock generator. [4]

Similar to the two-phase clock generator, the frequency of the clock is determined by the control signals and equation 2.8 which determines the value of the inductor and capacitors. The waveform of the control signals is shown in Figure 2.6.

$$4f = \frac{1}{2\pi\sqrt{LC}} \tag{2.8}$$

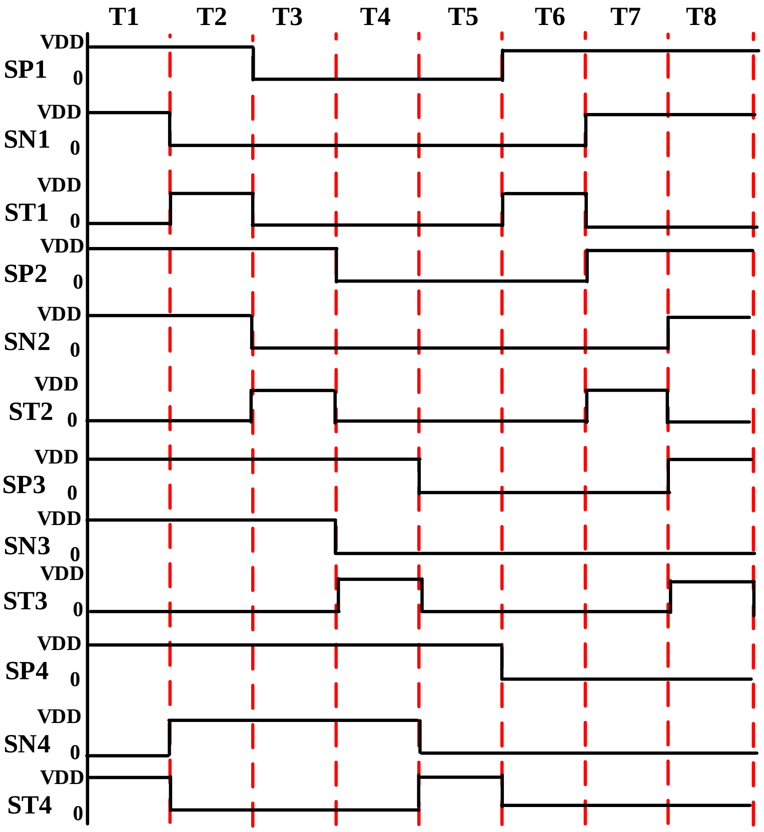


Figure 2.6: Control signals necessary to create a synchronous four-phase clock generator.

## 2.2 Correlation Power Analysis Attacks

There are three types of power analysis attacks: Simple (SPA), Differential (DPA), and Correlation. SPA attacks rely on visually inspecting power traces to steal the secret key which is not practical when basic defenses are implemented. DPA attacks use a difference of means approach to determine the secret key. The DPA attack has the disadvantage of increased noise and slow time to recover a secret key [53]. The Correlation Power Analysis Attack (CPA) is a powerful side-channel attack that can reveal a secret key used with an encryption circuit [54]. CPA attacks steal keys by correlating the dynamic power consumption of circuits with the input transitions and the encryption keys. To steal the secret key CPA attack finds relationships between power traces and hypothesized power model typically based on the Hamming Weight (HW) of the output.

### 2.2.1 CPA Attack Process

As mentioned previously, CPA attacks attempt to steal device information by correlating power consumption with a power model. One power model that is typically

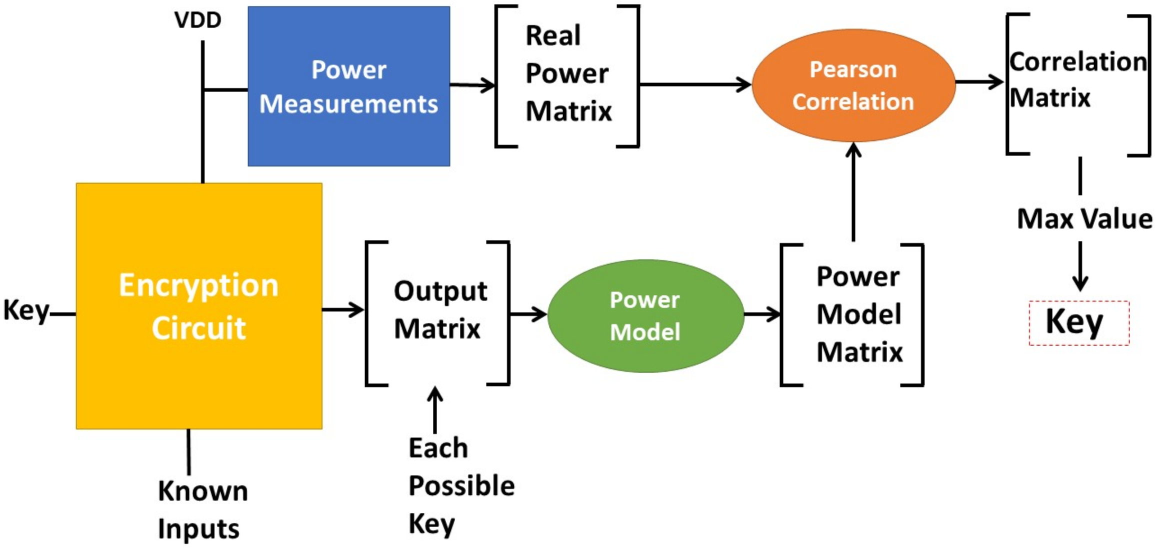


Figure 2.7: Correlation Power Analysis attack process.

used is the Hamming Weight (HW) power model. The HW defines the number of non-zero values in a binary string. For example, in the string 0011 1100, the HW would be 4. The theory behind using the HW model is that the number of 0's and 1's will strongly correlate with the power consumption of a circuit [53]. The correlation between the real power consumption and the power model can be calculated using the Pearson Correlation Coefficient which is defined in equation 2.9. Where COV(x,y) is the covariance between x and y and Var(x) is the variance of x. The Pearson equation will take in two data sets and determine if there is a linear relationship between the two data sets.

$$\rho(W,P) = \frac{COV(W,P)}{\sqrt{Var(W)}\sqrt{Var()}} \tag{2.9}$$

The steps to perform the Correlation Power Analysis Attack are shown in Figure 2.7 and are explained as follows.

1. Produce a cyphertext **O** from the output of an S-Box which takes in the plaintext **I** and the encryption key **K**. Let $I_i$ be an element in **I** where $i \in [0, d-1]$ and d is the number of plain texts. Let $K_j$ be an element in **K** where $j \in [0, k-1]$ where k is the number of possible keys for an S-Box circuit. For example, a 4-bit S-Box circuit has $2^4$ possible keys. Thus, the cyphertext should take the following form:
$$O_{i,j} = Sbox(I_i \oplus K_j) \tag{2.10}$$

2. Using the Hamming Weight model discussed previously, construct a hypothetical power model **HW** based on the output cyphertext **O**. Where HW takes the

form

$$HW_{i,j} = Hamming\_Weight(O_{i,j}) \tag{2.11}$$

3. Measure and record the real power traces for each input plain text **I**. The power consumption should be measured such that a data transition is occurring and thus we are measuring the dynamic power consumption. For example, if the input makes a transition at time t = 10ns then samples should be taken both before and after t = 10ns. The result of this step is a matrix of real power traces, $RP_{d,n}$ where n is the total number of samples taken.

4. Compare the **HW** matrix with the **RP** matrix using the Pearson Correlation Coefficient equation that was discussed previously. The comparison is made column by column for both the **HW** and **RP** matrix, each element produces a correlation value. We then can observe the largest value in the correlation matrix to determine which key-value best correlates with the power consumption.

### 2.2.2 Countermeasures Against CPA attacks

Various countermeasures have been proposed to defend against SPA, DPA, and CPA attacks since their inception. These defenses can be classified as either hiding or masking[40]. Hiding-based defenses look to remove the correlation between power consumption and input transition. One way this can be done is by making the power consumption uniform no matter what the input is. Masking involves randomizing the intermediate data values in the encryption circuit such that a correlation cannot be made with the original data and power.

Countermeasures can further be divided into whether they are circuit-level or algorithm-level countermeasures. Algorithm-based countermeasures are typically specific to an encryption algorithm and thus are difficult to automate the design flow. This thesis will focus on the circuit level countermeasures which can be standardized and used in any encryption algorithm.

#### CMOS based CPA-resistant logic styles

There have been various hiding-based CPA-resistant logic styles that have been proposed in the literature such as Sense-Amplifier-Based Logic (SABL) proposed by Tiri et al.[41]. SABL is based on the principles of dual-rail logic, a single switching event per cycle, and balanced capacitance networks. The major drawback of SABL is that an unbalanced capacitance load can lead to data being correlated with power consumption. This is common as it is difficult to balance capacitance on different interconnects due to process variations and different fan-outs. Tiri et al. also proposed Wave Dynamic Differential Logic (WDDL)[55] which is a logic design that can be created using standard cells which is beneficial to the standard and ASIC design flow. There are many drawbacks that accompany WDDL such as the large area required, the increased power consumption, differential routing, and the restriction to only AND and OR gates [56].

There have also been many masking circuit-level techniques proposed in the literature. Popp and Mangard have proposed Masked Dual-Rail Pre-Charge Logic (MDPL)[57] which is a dual-rail logic using majority gates with masked inputs. The basic idea behind MDPL is to use a True Random Number Generator (TRNG) and a Pseudo-Random Number Generator (PRNG) block to produce a masked input and an inverse masked input. The masked values are then used as inputs to a majority gate to produce a AND value and the inverse masked values are used as inputs to a second majority gate to produce a NAND value. There are some drawbacks to using MDPL such as the extra area and power overhead necessary to create the masked values. Further, MDPL can only create AND and NAND gates and thus other gates must be created using those gates. Another masked logic is the Dual-Rail Random Switching Logic (DRSL)[58] which is similar to MDPL in that it is a dual-rail logic that utilizes masked inputs to remove the correlation with the power consumption. In the case of both MDPL and DRSL, it has been shown that they are both still vulnerable to power analysis attacks by attacking the flip-flops used within the logic circuits [59].

### Adiabatic based CPA-resistant logic styles

Adiabatic logic is a low-energy design technique that utilizes time-varying voltage sources to reduce the energy consumption of circuits. Adiabatic logic circuits can also be designed in such a way that they are resistant to power analysis attacks.

Secure Adiabatic Logic (SAL) is an adiabatic logic design that creates energy-efficient and CPA-resistant circuits [60]. A major drawback of SAL is that it requires eight separate clocks to operate. The interconnection area and clock design for an eight-clock network are very difficult and thus not practical for implementation in IoT devices. Numerous four-phase adiabatic logic designs have been implemented as CPA-resistant circuits. Symmetric Adiabatic Logic (SyAL)[61] was created by Choi et al by modifying an existing adiabatic architecture known as efficient charge recovery logic (ECRL) [62]. The idea behind SyAL involves creating a FET network such that the number of transistors that are off and on is balanced in each network. Further, a bridge FET is added so that the supply current is not affected by previous data. Charge-Sharing Symmetric Adiabatic Logic (CSSAL) [63] is another adiabatic circuit proposed by Monteiro et al. also utilizes the idea of charge sharing to create a CPA-resistant circuit. The operation of CSSAL involves using a bridge transistor to charge share between the dual outputs and a discharge transistor to discharge the internal capacitance to ground. Kumar et al. have presented a low-energy, CPA-resistant adiabatic logic circuit known as Energy-Efficient Secure Positive Feedback Logic (EE-SPFAL) [64]. The proposed circuit is a modified implementation of another adiabatic logic family known as Positive Feedback Adiabatic Logic[65]. The basis of EE-SPFAL is that the evaluation networks are balanced such that the number of transistors that are on is equal. Further, discharge transistors are used to ensure that all internal capacitances are discharged to ground at the end of each cycle. One issue common among the four-phase CPA-resistant adiabatic circuits is that the clock generator and interconnect networks are complex and thus difficult to implement in the chip design flow.

### 2.2.3 Quantifying a Circuits Resistance Against Power Analysis Attacks

It is important to quantify a circuit's resistance against power analysis attacks in order to properly compare various proposed countermeasures. To that end, we introduce two common proposed metrics used in the literature to compare circuit-level countermeasures against power analysis attacks. The two metrics discussed include Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD).

#### Normalized Energy Deviation

NED is a metric used to quantify how much the power consumption varies depending on the input transitions. NED can be defined as

$$NED = \frac{E_{max} - E_{min}}{E_{max}} \tag{2.12}$$

NED determines the normalized difference between the minimum and maximum power consumption. For example, a 2-input logic gate has 16 possible input transitions (0-0, 0-1, 1-1, 1-0 for each input), and each transition results in different power consumption. NED takes the max and min of those power consumption and determines the normalized difference. This metric tells us how much the power consumption varies within a circuit. The ideal NED value would be 0 which would represent no change in the power consumption.

#### Normalized Standard Deviation

NSD is another metric used to determine how resilient a circuit is against power analysis attacks. NSD can be defined as

$$NSD = \frac{\sigma_e}{\overline{E}} \tag{2.13}$$

Where $\sigma_e$ is the standard deviation of the power consumption and $\overline{E}$ is the average energy consumption. NED only uses the max and min power consumption while NSD utilizes each of the power consumption that results from each input transition. The lower the power variation, the lower the standard deviation will be, and thus the more a circuit will theoretically be secure against power analysis attacks.

## 2.3 Magnetic Tunnel Junctions (MTJ) and hybrid CMOS/MTJ circuits

### 2.3.1 Magnetic Tunnel Junctions

Magnetic Tunnel Junctions (MTJ) are non-volatile spintronic-based memories. The structure of MTJs consists of two ferromagnetic (FM) layers and a thin oxide layer that separates the two FM layers [66]. For MTJs to act as storage elements, one of the FM layers is fixed to a certain magnetization (referred to as the fixed layer) while

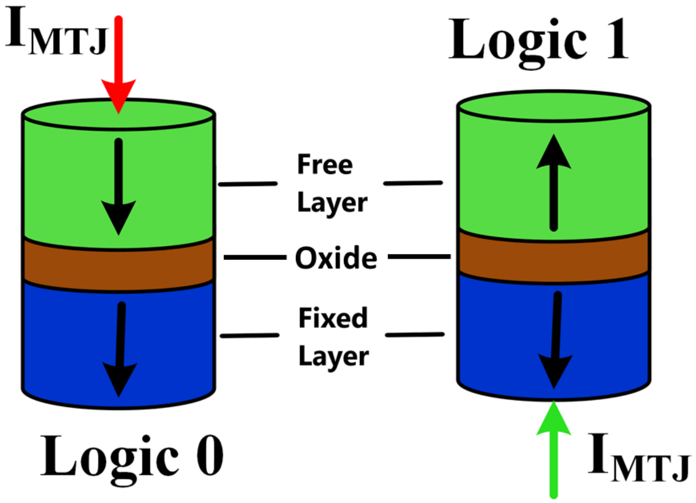


Figure 2.8: Structure of Magnetic Tunnel Junction with Spin Transfer Torque (STT) switching.

the remaining layer (referred to as the free layer) is free to take either a parallel or anti-parallel magnetization with respect to the fixed layer [67].

This can be seen in Figure 2.8 as the bottom layer of the MTJ is fixed and the top layer is free to take a direction either parallel or anti-parallel to the fixed layer. Information is stored in the form of resistance differences between the two orientations of the MTJ. If the MTJ shows a parallel magnetization ($R_P$) then it will have lower resistance than when it has an anti-parallel magnetization ($R_{AP}$) [68]. The parallel resistance can be determined by equation 2.14. An important property of MTJs is the tunnel magnetoresistance ratio (TMR) which is given as $TMR = (R_{AP} - R_P)/R_P$. MTJs with higher TMR have been shown to have greater reliability and implementation capability in high-speed MRAM [69, 70]. Table 2.1 contains the MTJ device parameters used to describe the MTJs functionality [11]. In Table 2.1, $\sigma$ represents a variable that follows a Gaussian distribution with $\sigma = 3\%$.

$$R_p = \frac{t_{ox}}{F \cdot \overline{\psi}^{\frac{1}{2}} \cdot Area} \cdot exp(coef \cdot t_{ox} \cdot \overline{\psi}^{\frac{1}{2}}) \qquad (2.14)$$

### 2.3.2 Hybrid CMOS/MTJ Circuits

Logic-in-Memory (LiM) is a promising solution to reduce the energy and delay of circuits. LiM looks to reduce delay and energy by placing the logic and memory in the same blocks to avoid the long interconnects between logic and memory that are typically found. For LiM to come to fruition, the memory portion should be non-volatile, have low read/write latency, and should have a strong endurance [71]. All of these characteristics are found within MTJs which makes them a promising choice for LiM applications. The structure of the LiM is shown in Figure 2.9. The

Table 2.1: Magnetic Tunnel Junction parameters used in simulations [11]. $\sigma$ represents a parameter that follows a Gaussian distribution with $\sigma = 3\%$.

| **Parameter** | **Description** | **Value** |
|---|---|---|
| $t_{sl}$ | Thickness of free layer | $\sigma$1.3nm |
| a | Length of surface long axis | 40nm |
| b | Width of surface short axis | 40nm |
| $t_{ox}$ | Thickness of the Oxide barrier | $\sigma$0.85nm |
| TMR | Tunnel Magnetoresistance ratio | $\sigma$200% |
| RA | Resistance Area Product | 5 $\Omega\mu^2$ |
| Area | MTJ layout surface | 40nm x 40nm x $\frac{\pi}{4}$ |
| $R_p$ | Parallel resistance | 6.21 k$\Omega$ |
| $R_{ap}$ | Anti-parallel resistance | 18.64 k$\Omega$ |

structure consists of a Pre-Charged Sense Amplifier (PCSA) which is used to sense the resistance differences in the MTJs. Further, it consists of a dual-rail CMOS logic network and a writing circuit to switch the MTJs by applying a current greater than the switching current of the MTJs.

There have been numerous LiM CMOS/MTJ circuits proposed in the literature. Deng et al. have proposed a low-power CMOS/MTJ full adder and various logic gates that follow the standard structure shown in Figure 2.9 [5]. The circuit consists of a pre-charged sense amplifier, evaluation transistors, and two MTJs set in complementary states. Deng et al. proposed XOR/XNOR circuit is shown in Figure 2.10. Following the same implementation structure, many other circuits have been proposed. Barla et al. have proposed an Arithmetic Logic Unit (ALU) based on the principles of CMOS/MTJ circuits [72]. The proposed design is able to perform addition and logical operations which can be selected by predefined Opcodes.

One of the major issues with CMOS/MTJ circuits is that the switching of the MTJs consumes substantial power and thus can allow an adversary to perform a power analysis attack on the circuit[73]. Kumar et al. proposed a modification of the CMOS/MTJ circuit proposed by Deng et al [73]. The modified circuit adds a transistor that cuts off supply to VDD when MTJs are being written to. This ensures that information is not leaked when MTJs are switched and thus the circuit consumes uniform power consumption. The drawback of this proposed design is that the transistors used to pre-charge the outputs must be up-sized to ensure correct operation which leads to added area.

## 2.4 Physically Unclonable Functions

Physically Unclonable Functions (PUF) can be thought of from a high-level perspective as a block box that takes in an input and outputs a specific random value. The inputs into a PUF are known as challenges and the outputs of the PUF are known as responses, this forms a challenge-response pair (CRP) for each PUF. The idea of

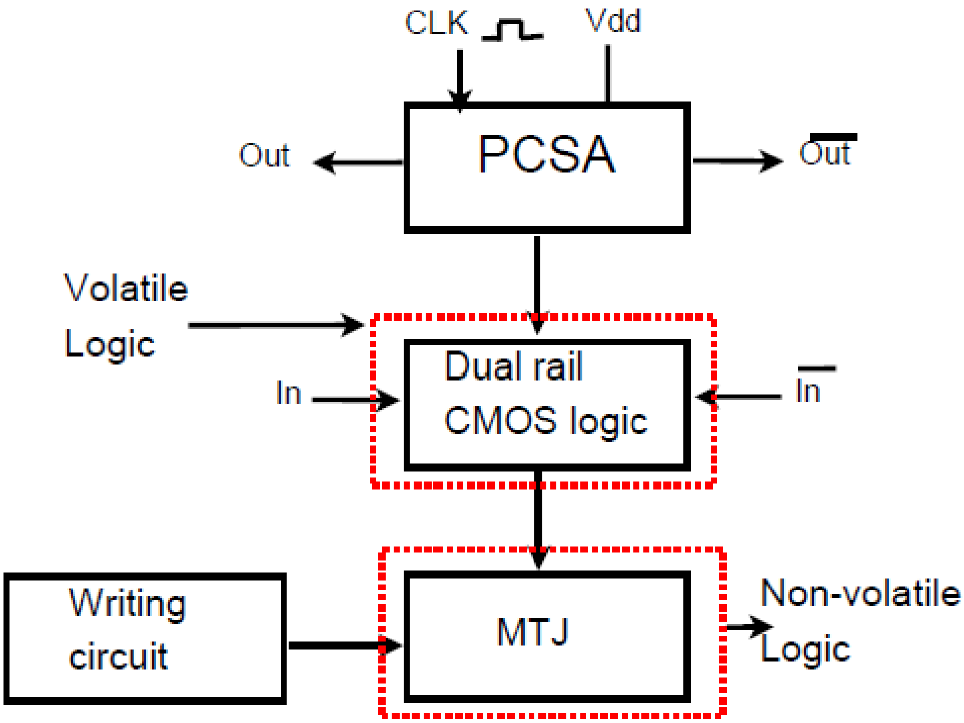


Figure 2.9: General structure of Hybrid CMOS-MTJ circuits (© 2021 IEEE).

PUF generation is exemplified in Figure 2.11. Even if two PUFs are theoretically the same, the outputs should theoretically be different. This is because the basic idea behind PUFs is they use process variation that exists between different devices to give the device a unique digital fingerprint. For example, the threshold voltage between two "identical" transistors will be slightly different from chip to chip because of the variation that occurs during fabrication. PUFs can be classified into two categories, strong and weak. Strong PUFs are PUFs that have a large number of CRPs while weak PUFs have a limited number of CRPs. Both strong and weak PUFs should be designed such that there is a small likely hood that two responses are the same.

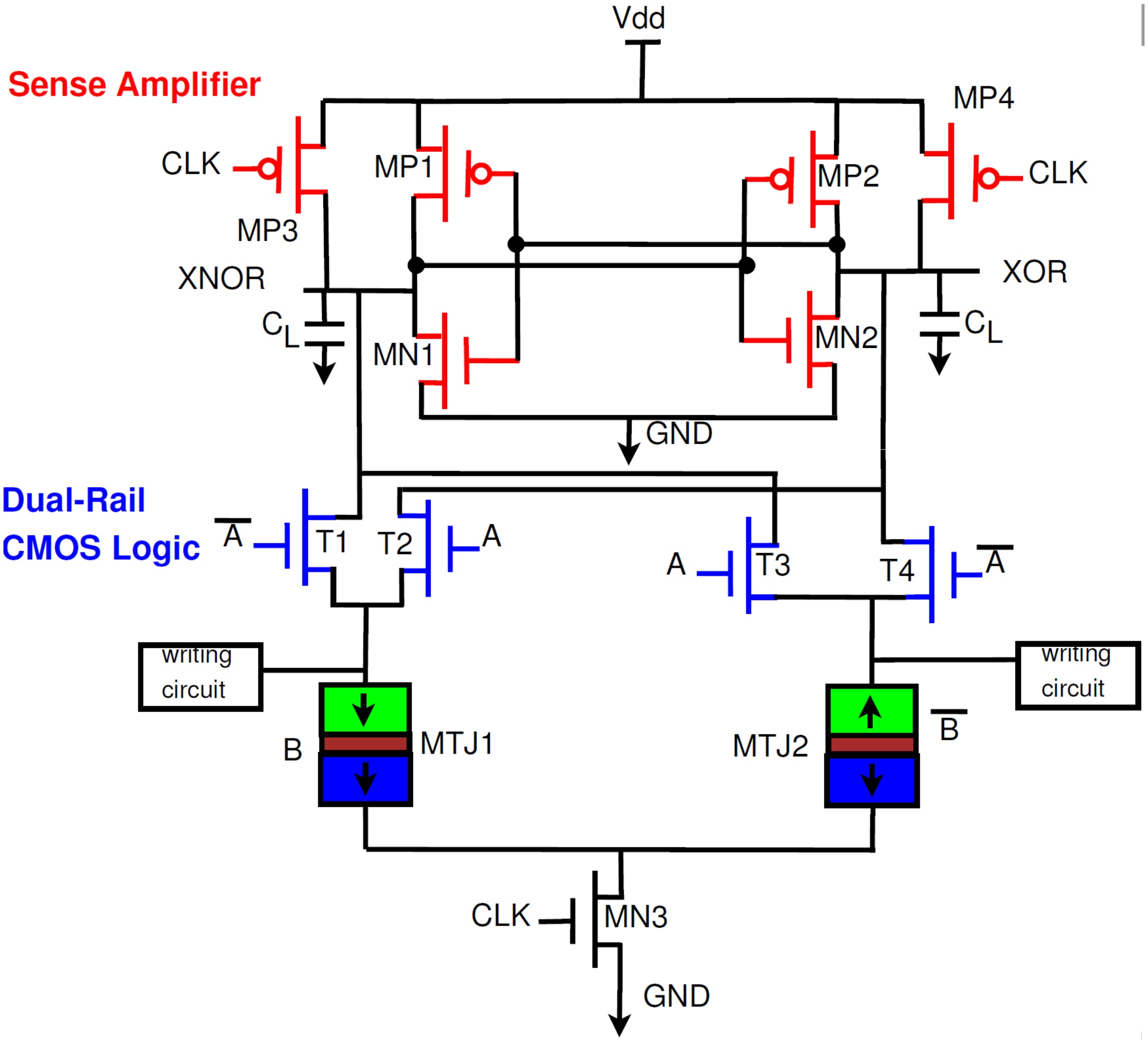


Figure 2.10: Example of hybrid CMOS/MTJ circuit [5].

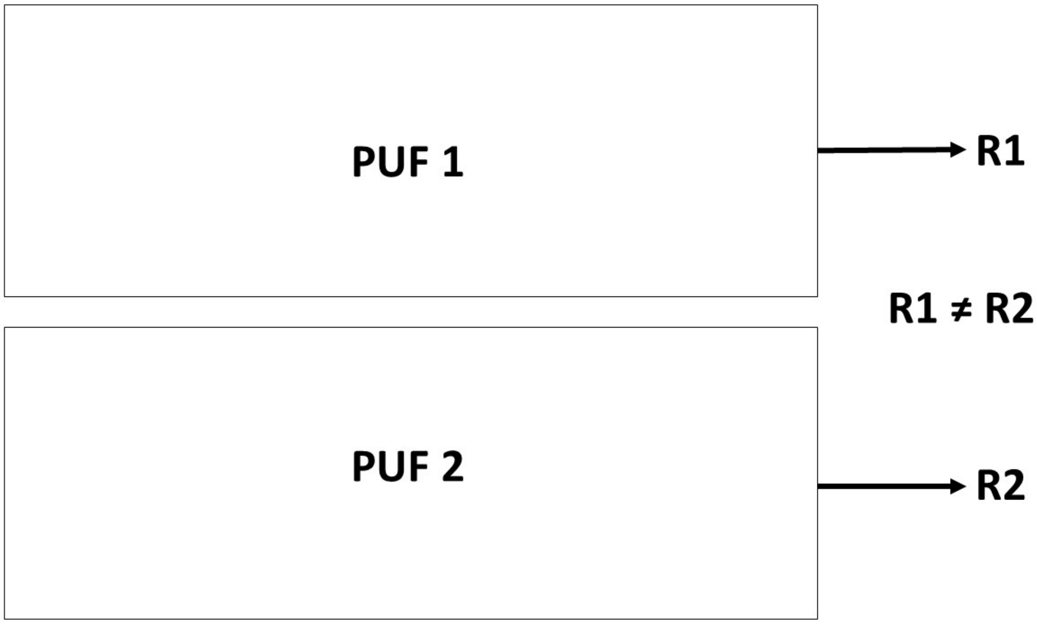


Figure 2.11: Identical PUFs result in different responses.

### 2.4.1 PUF Evaluation Metrics

It is important to validate the security of our proposed PUF using metrics common to other proposed PUFs. To that end, we introduce three standardized metrics that are common in literature for evaluating the effectiveness of the PUFs: uniqueness, uniformity, and reliability [74, 75].

#### Uniqueness

The uniqueness of a PUF is used to determine how different one PUF instance is from another. The ideal uniqueness value is 50%. Uniqueness is defined as

$$Uniqueness = \frac{k}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{K} \frac{HD(R_i, R_j)}{n} \cdot 100 \tag{2.15}$$

Where $R_i$ and $R_j$ are two different PUF instances, HD is the hamming distance between the two instances, k is the number of PUF instances, and n is the bit length of the PUF response. In our testing, we use k = 200 and n = 128.

#### Uniformity

Uniformity tells us the number of 0's and 1's in a PUF response. An ideal uniformity is 50% which reflects an equal number of 0's and 1's in the response. Uniformity is defined as

$$Uniformity = \frac{1}{n \cdot k} \sum_{i=1}^{k-1} r_{i,l} \cdot 100 \tag{2.16}$$

Where n is the bit length of the response, k is the number of PUF instances, and $r_{i,l}$ is the $l^{th}$ bit from the instance i.

### Reliability

Reliability tells us how the PUF response changes as environmental parameters change such as temperature and supply voltage. Reliability is defined as

$$Reliability = 100 - \frac{1}{k} \sum_{i=1}^{k} \frac{HD(R_i, R^{'}_{i,t})}{n} \tag{2.17}$$

$R_i$ is the response of a golden PUF that is used as a comparison to determine how much the response has changed. $R^{'}_{i,t}$ is the response of the PUF that is affected by the environmental change. The ideal value of reliability is 100% which represents no changes between the golden PUF and the PUF in non-ideal conditions.

## 2.4.2 PUF Design Taxonomy

Various PUFs have been proposed in the literature, Figure 2.12 shows the taxonomy of PUFs and example PUFs that make up the taxonomy. The majority of PUFs are contained within the Silicon PUF class. Further, the focus of this thesis will also be on silicon-based PUFs.

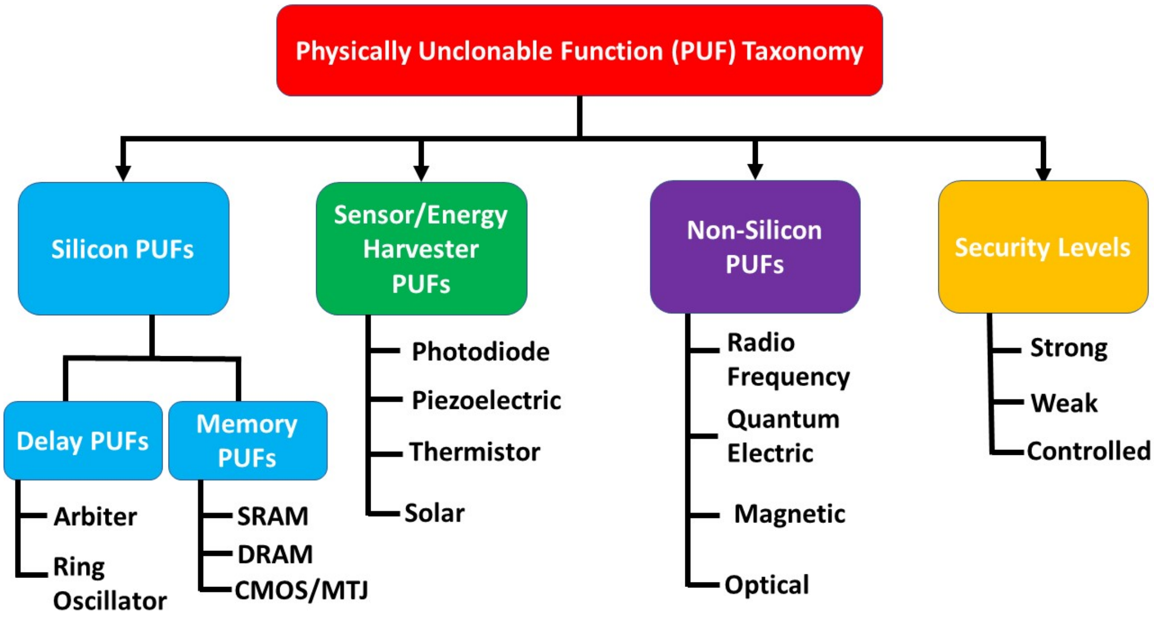


Figure 2.12: PUF taxonomy.

Silicon PUFs can typically rely on manufacturing variation that typically result in variations of gate delays and threshold volatages of the transistors. Silicon PUFs can take many forms such as the arbiter [76, 76], ring oscillator [77], SRAM [6], butterfly[6], latch [48], and flip-flop [78]. The aforementioned PUFs will now be briefly described.

1. **Arbiter** The arbiter PUF is a silicon PUF that relies on gate delay variation because of process variation to produce a response. The structure of the arbiter PUF consists of two delay paths of theoretically equal lengths. Due to gate delay variation, one of the paths will have a slightly lower delay and thus will produce a response of 0 or 1. One of the main drawbacks of the arbiter PUF is it is difficult to design multiple circuits with equal delay paths which are important for the functionality of the arbiter PUF.

2. **Ring Oscillator** The ring oscillator PUF is a weak PUF that also uses the variation in gate delay to generate a response. The basis of ring oscillator PUFs is that multiple instances are created and as a result of gate delay, the instances will have varying frequencies. These frequencies are compared to generate a response bit. A drawback of ring oscillator PUFs is that environmental changes affect the frequency of the ring oscillators and thus the reliability is lowered.

3. **SRAM** The SRAM PUF is a weak PUF that utilizes variation in the threshold voltage to generate a response. The structure of the SRAM PUF is shown in Figure 2.13. On startup, the two PMOS transistors that make up the SRAM will begin charging, however, one of the FETs will have a lower threshold voltage and thus charge faster than its counterpart. This will cause one of the outputs to be pulled to logic 1 and the other output to logic 0.

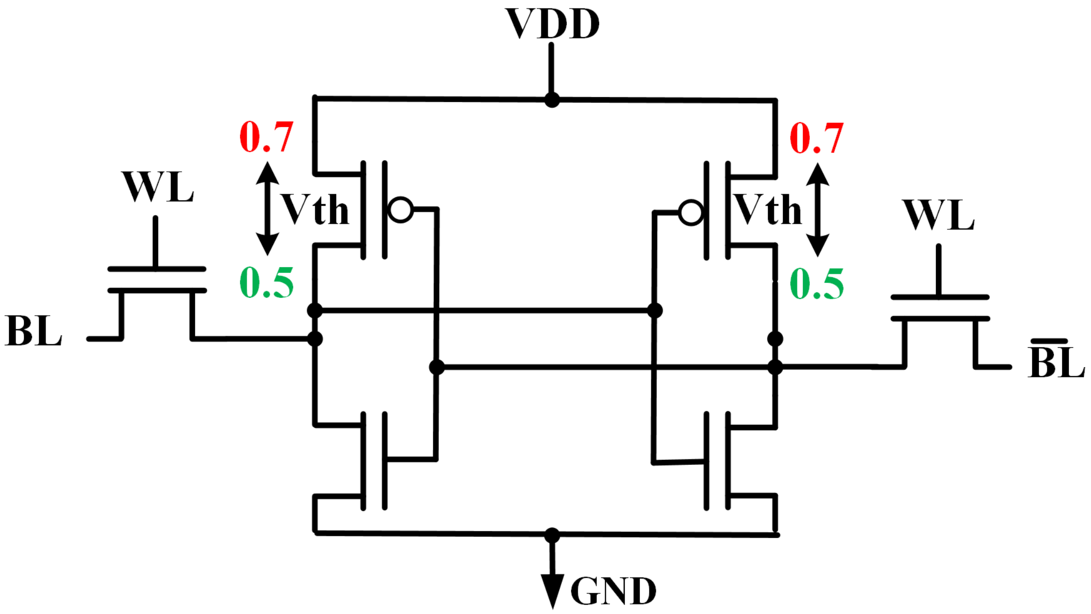


Figure 2.13: CMOS SRAM-based PUF where $V_{th}$ changes because of process variations. [6].

# Chapter 3

# 2-Phase Energy-Efficient Secure Positive Feedback Logic

Dynamic power consumption is one of the major sources of power consumption within an integrated circuit. Dynamic power consumption becomes a major issue in area and battery-contained devices such as IoT devices. Thus, in this chapter, we look to reduce the dynamic power consumption and create a CPA-resistant circuit through the use of adiabatic logic. Adiabatic logic is a low-energy design technique that utilizes energy recovery principles through time-varying clocks. This chapter presents our work on 2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL). 2-EE-SPFAL utilizes a two-phase power clock to reduce the dynamic energy consumption of a circuit. Further, 2-EE-SPFAL is designed in such a way that it is resistant to CPA attacks. In this chapter, we show that 2-EE-SPFAL saves between 76.5% and 21.3% energy consumption at frequencies between 100kHz and 25MHz when compared with its CMOS counterpart. Further, we demonstrate that 2-EE-SPFAL is secure against power analysis attacks by performing a CPA attack on an encryption circuit implemented with 2-EE-SPFAL. The key could not be recovered when using 2-EE-SPFAL, however, when using CMOS the key could be stolen.

The research work presented in this chapter was previously published in [7] as Kahleifeh, Zachary, and Himanshu Thapliyal. "Adiabatic logic based energy-efficient security for smart consumer electronics." IEEE Consumer Electronics Magazine 11.1 (2020): 57-64., © 2020 IEEE.

## 3.1 2-EE-SPFAL: PROPOSED 2-PHASE ENERGY EFFICIENT SECURE POSITIVE FEEDBACK LOGIC

Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) is a recently proposed low energy and CPA resistant logic family [64]. Figure 3.1 shows the general structure of a 2-EE-SPFAL adiabatic circuit. The structure consists of two balanced evaluation networks. The structure also consists of cross-coupled inverters acting as a sense amplifier. Finally, the discharge transistors are used to reset the output so that the power consumption remains uniform. EE-SPFAL was originally constructed with a 4-phase trapezoidal clocking scheme. In this chapter, we present the 2-phase design of EE-SPFAL using sinusoidal power clocks. For 2-phase EE-SPFAL to work properly and be CPA resistant, adjustments are made to the clocking scheme and discharge signals.

Figure 3.2 shows the proposed sinusoidal clocking scheme. It consists of two

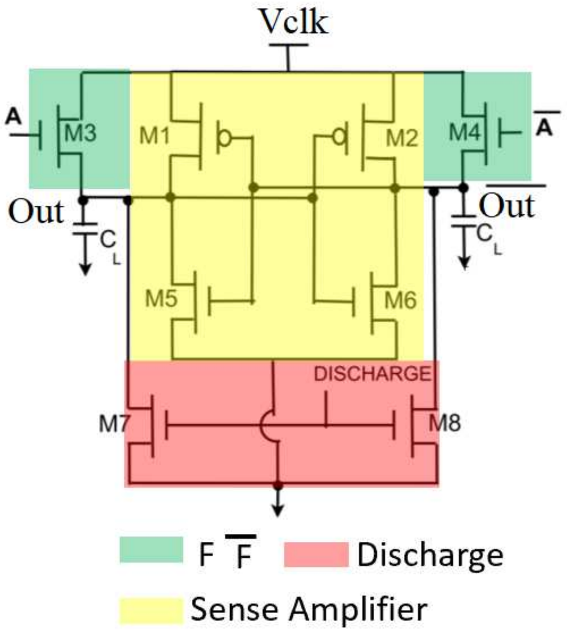


Figure 3.1: General structure of 2-EE-SPFAL circuit (© 2022 IEEE).

sinusoidal waves 180° out of phase. The clocking scheme consists of an "evaluate" phase in which the power clock is rising and a "recover" phase in which the power clock is falling. There are two discharge signals, one for each clock. The period and delay of the discharge signals are equal to their respective clocks.

Using two clocks rather than four results in multiple benefits. Namely, two clocks reduce the amount of area and complexity required to generate the power clock. Take the 4-phase clock generator in [4] and the 2-phase clock generator in [79] as a case study. The 4-phase design consumes a substantial area and requires a more complex design than the 2-phase design.

The 4-phase clocking scheme also leads to a more complicated routing scheme. Using 4-phases requires four separate interconnects when four or more gates are cascaded. Take the four buffers seen in Figure 3.3a as a case study, in the 4-phase case, eight separate interconnects are required for the circuit to operate correctly while in the 2-phase case only four interconnects are needed.

## 3.2 2-Phase Adiabatic Power Clock Generator

This section discusses the energy-efficient adiabatic Power Clock Generator (PCG) which is used to operate 2-EE-SPFAL. The PCG uses an external inductor and the load of the adiabatic circuit to generate the waveforms. There are many existing clock generators, for this case study, we have used the 2N-2P synchronous clock generator discussed in [3]. The timing diagram of the controlling external signals is shown in Figure 3.4. From Figure 3.4, we developed the novel way for discharge and $\overline{discharge}$ signals to have dual-function: (i) control signals for the clock generator, and (ii)

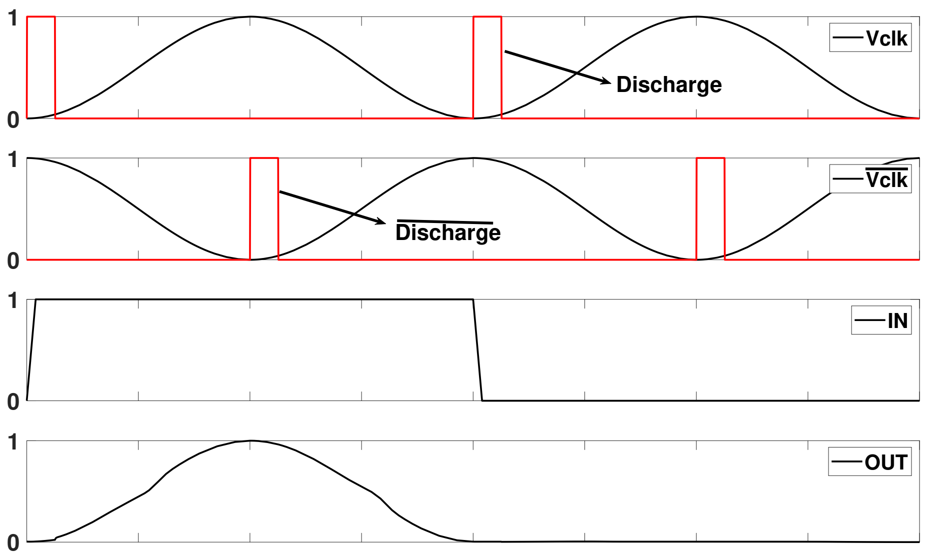
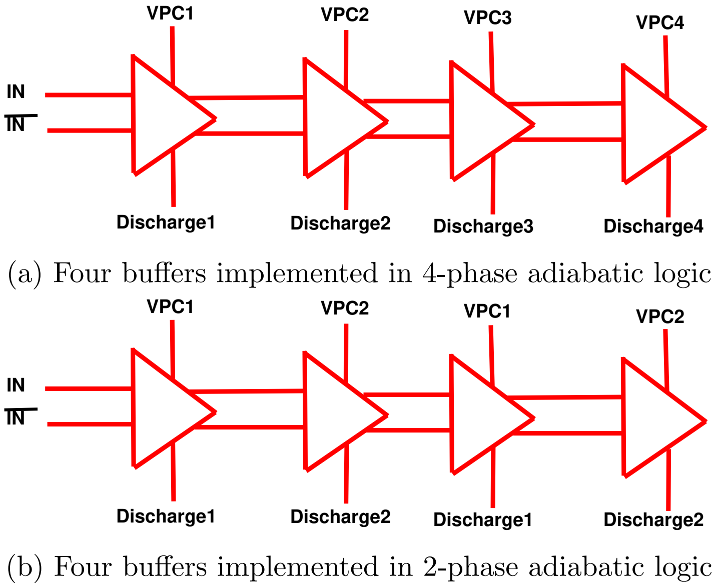


Figure 3.2: Proposed 2-phase sinusoidal clocking scheme for 2-EE-SPFAL (© 2022 IEEE).



(a) Four buffers implemented in 4-phase adiabatic logic.

(b) Four buffers implemented in 2-phase adiabatic logic.

Figure 3.3: Design of four buffers using 4-phase clocking and 2-phase clocking (© 2022 IEEE).

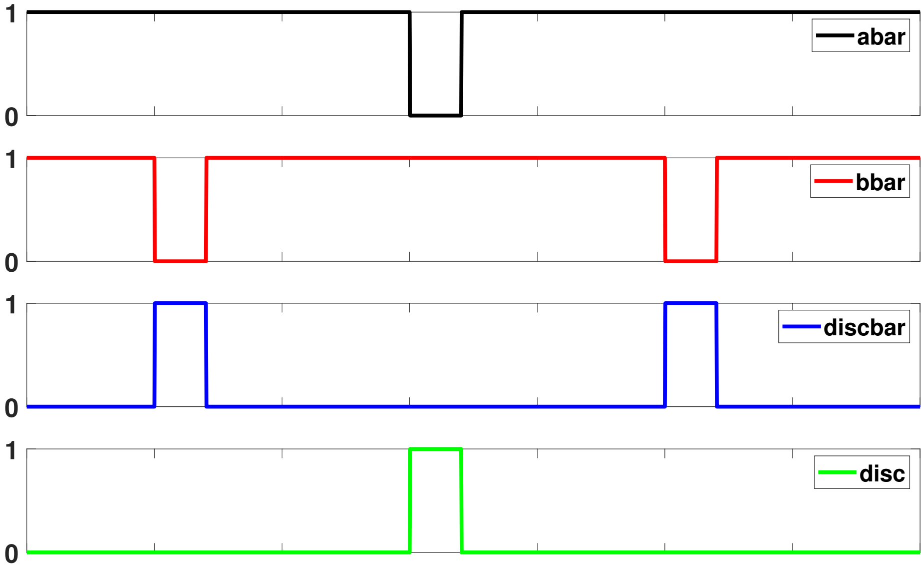


Figure 3.4: Synchronous 2N-2P 2-phase clock supporting control signals (© 2022 IEEE).

discharge control for the adiabatic logic circuit. The proposed dual-function reduces the number of external signals necessary for operation.

### 3.3 Demonstration of 2-EE-SPFAL Security and Energy Efficiency

Each 2-EE-SPFAL gate results in a half-cycle delay. Thus, additional buffers are inserted in 2-EE-SPFAL circuits to synchronize the outputs.

We evaluate two criteria to determine the energy efficiency and security of 2-EE-SPFAL. The criteria Normalized Energy Deviation (NED) is defined as ($E_{max}$ - $E_{min}$)/$E_{max}$. NED is used to indicate the percent difference between the minimum and maximum energy consumption of the possible input transitions. A second parameter, Normalized Standard Deviation (NSD), is defined as $\frac{\sigma_e}{\overline{E}}$ where $\sigma_e$ is the standard deviation of the energy dissipated by the circuit per input transition and $\overline{E}$ is the average energy dissipation. Both NED and NSD are important parameters when determining circuit resilience to CPA attacks. NED and NSD values reported in this chapter are calculated with the integration of the power clock generator.

Table 3.1 show the simulated and calculated parameters for the 2-EE-SPFAL NAND and XOR implementation at 12.5 MHz with the integrated clock generator. The low NED and NSD calculations show that 2-EE-SPFAL has minimal energy consumption changes between the input transitions. From Table 3.1, it can also be seen that the XOR gate of 2-EE-SPFAL has lower values of NED and NSD compared to the NAND gate.

From Figure 3.5, we can observe that regardless of input combination, the current

Table 3.1: Simulation and calculation results for NAND and XOR gates.

| Parameter | 2-EE-SPFAL (NAND) | 2-EE-SPFAL (XOR) |
|---|---|---|
| $E_{min}(fJ)$ | 2.94 | 2.86 |
| $E_{max}(fJ)$ | 3.02 | 2.87 |
| $E_{avg}(fJ)$ | 2.99 | 2.87 |
| NED (%) | 2.6 | 0.21 |
| NSD (%) | 0.75 | 0.08 |

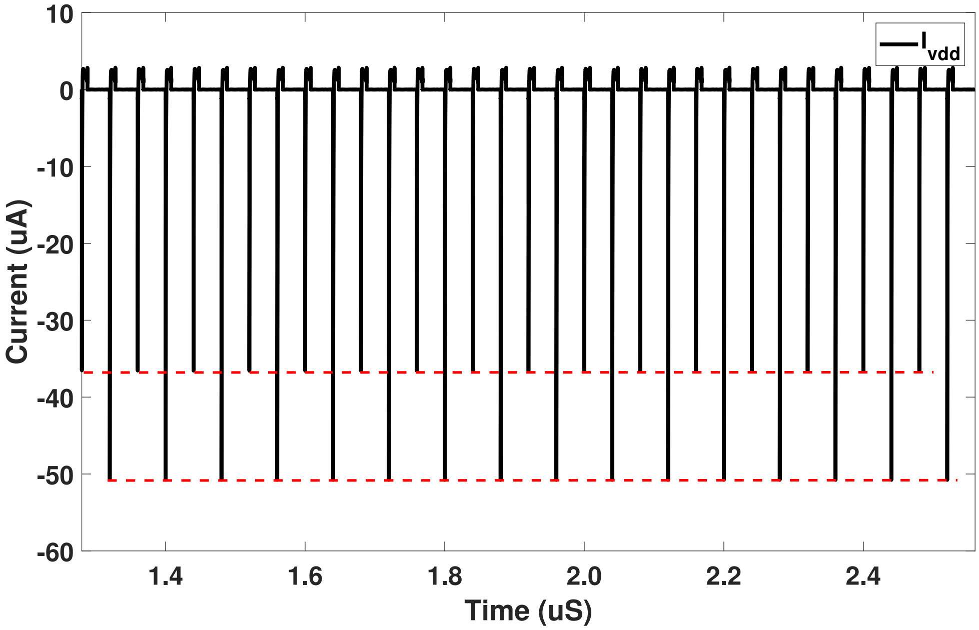
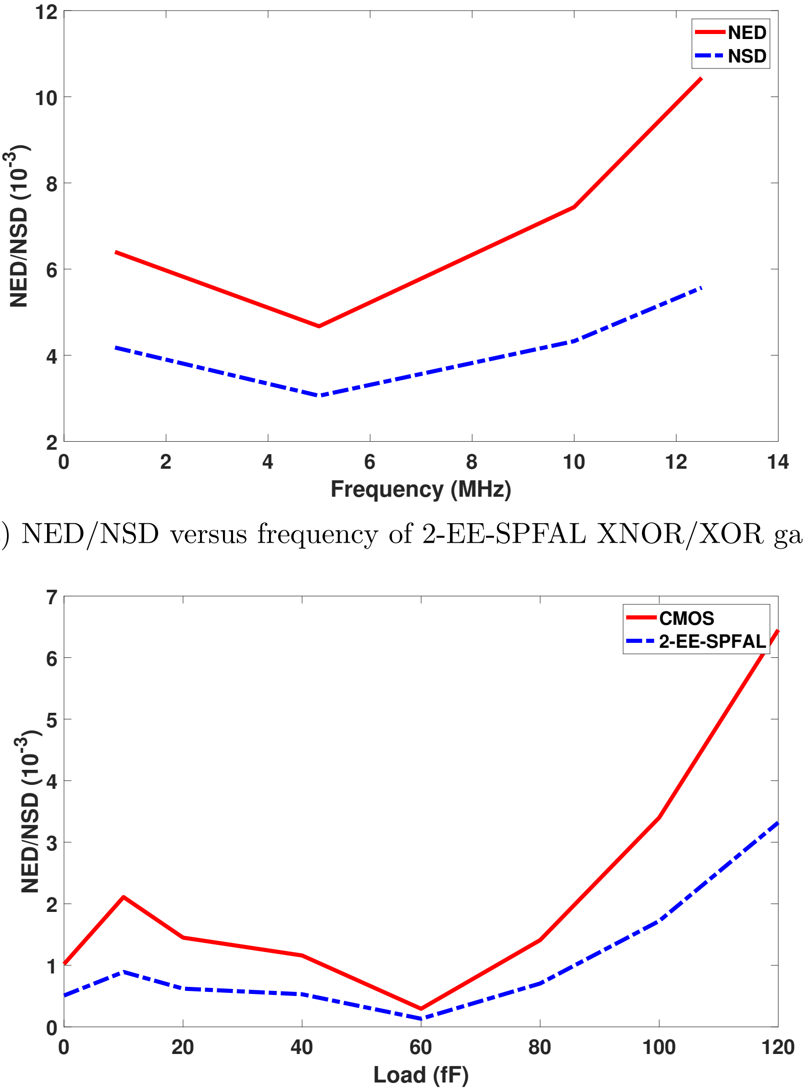


Figure 3.5: Uniform current consumption of the 2-EE-SPFAL XOR gate (© 2022 IEEE).

consumption of the XOR gate is nearly constant. The small variations in current results in minimal NED and NSD values and thus are theoretically more resistant to Correlation Power Analysis (CPA) attacks.

Furthermore, we examined the relationship between NED/NSD, frequency, and output load values. The relationships can be seen in Figures 3.6a and 3.6b. We can observe that as frequency increases NED/NSD values also increase. The same relationship can be seen between NED/NSD and load. As the output load surpasses 60 fF the NED/NSD values begin to increase. When designing circuits one should take into consideration these relationships to prevent information leakage.



(a) NED/NSD versus frequency of 2-EE-SPFAL XNOR/XOR gate.

(b) NED/NSD versus load of 2-EE-SPFAL XNOR/XOR gate.

Figure 3.6: Relationship between NED/NSD, frequency, and load for 2-EE-SPFAL XOR/XNOR gate (© 2022 IEEE).

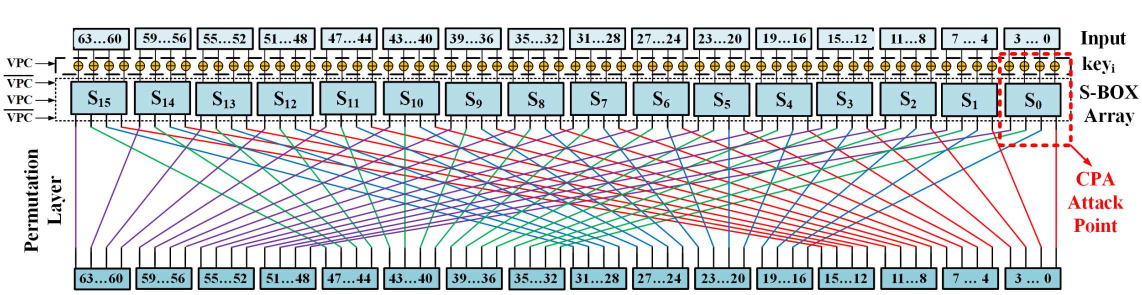


Figure 3.7: One round of PRESENT-80 implemented in 2-EE-SPFAL.

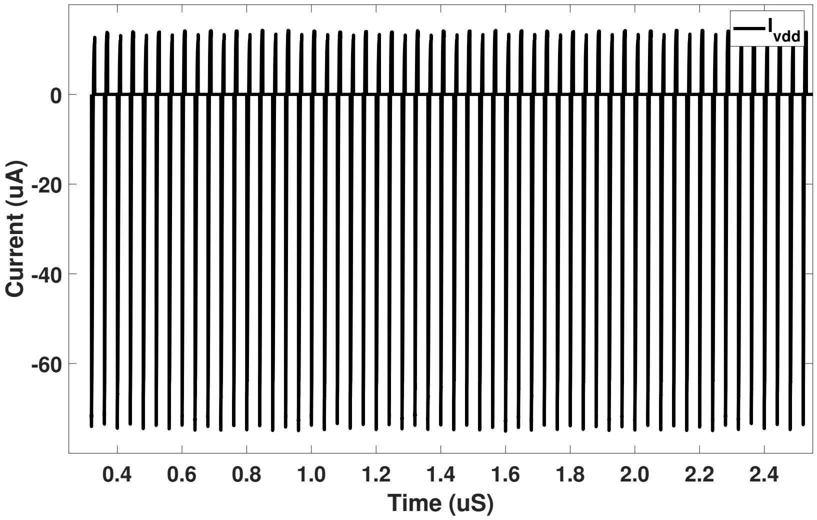


Figure 3.8: Uniform current traces of PRESENT-80 implemented with 2-EE-SPFAL and clock generator (© 2022 IEEE).

## 3.4 A Specific Case Study on PRESENT-80

### 3.4.1 PRESENT: A lightweight encryption

PRESENT [80] is a lightweight cipher. PRESENT has low area overhead which makes it an ideal candidate for smart electronic circuits that look to balance area and security. PRESENT supports key lengths of 80 or 128 bits. As the goal of this chapter is low energy, we decided to use an 80-bit key.

PRESENT-80 implemented in CMOS is susceptible to side-channel attacks such as Correlation Power Analysis (CPA). Many countermeasures against CPA attacks are not suitable for smart electronic devices as they consume large amounts of power thus we explore designing PRESENT-80 using 2-EE-SPFAL.

### 3.4.2 2-EE-SPFAL Implementation of PRESENT-80

CMOS implementation of PRESENT-80 is susceptible to Correlation Power Analysis (CPA) attacks and consumes large amounts of energy and thus is not suitable for low power smart electronic devices. In this section, we discuss the implementation of one round of PRESENT-80 with 2-EE-SPFAL. 2-EE-SPFAL requires two sinusoidal clocks 180° out of phase. Figure 3.7 shows the implementation of 1-round of PRESENT 80. The AddRoundKey stage is operated by $\phi_1$, the S-Box stage consists of both $\phi_1$ and $\phi_2$ where $\phi_1$ and $\phi_2$ are the two respective power clocks.

PRESENT-80 implemented with 2-EE-SPFAL and an integrated clock generator leads to more secure operation from uniform current consumption as seen in Figure 3.8. The uniform current traces during the operation of PRESENT-80 will prevent information leakage as we will see when a Correlation Power Analysis is performed. Figure 3.9 and Table 3.2 show the energy per cycle of both the CMOS and 2-EE-

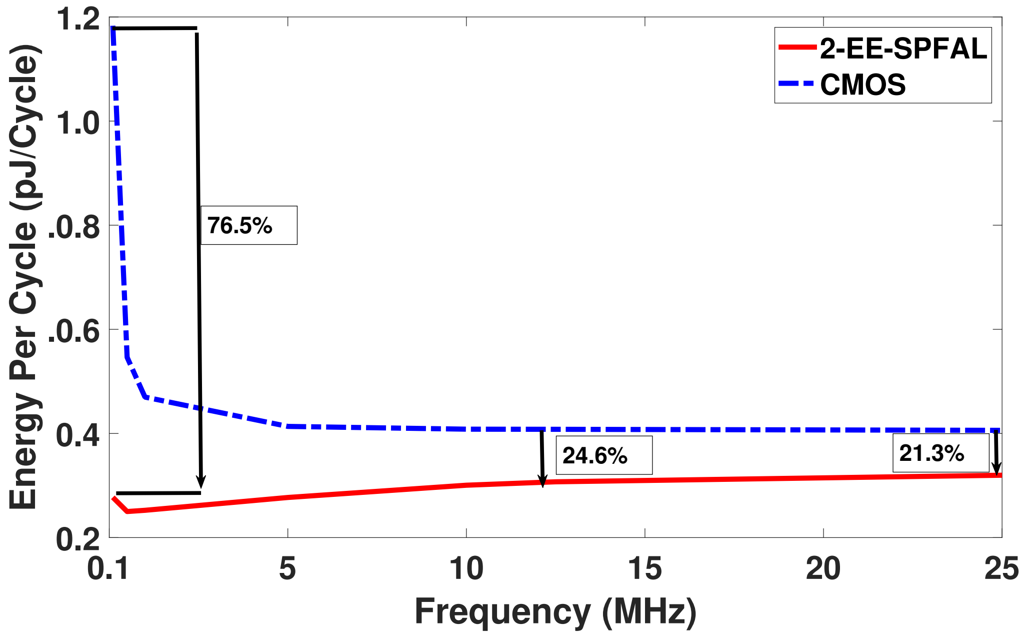


Figure 3.9: Energy per cycle of PRESENT-80 implemented in CMOS and 2-EE-SPFAL (© 2022 IEEE).

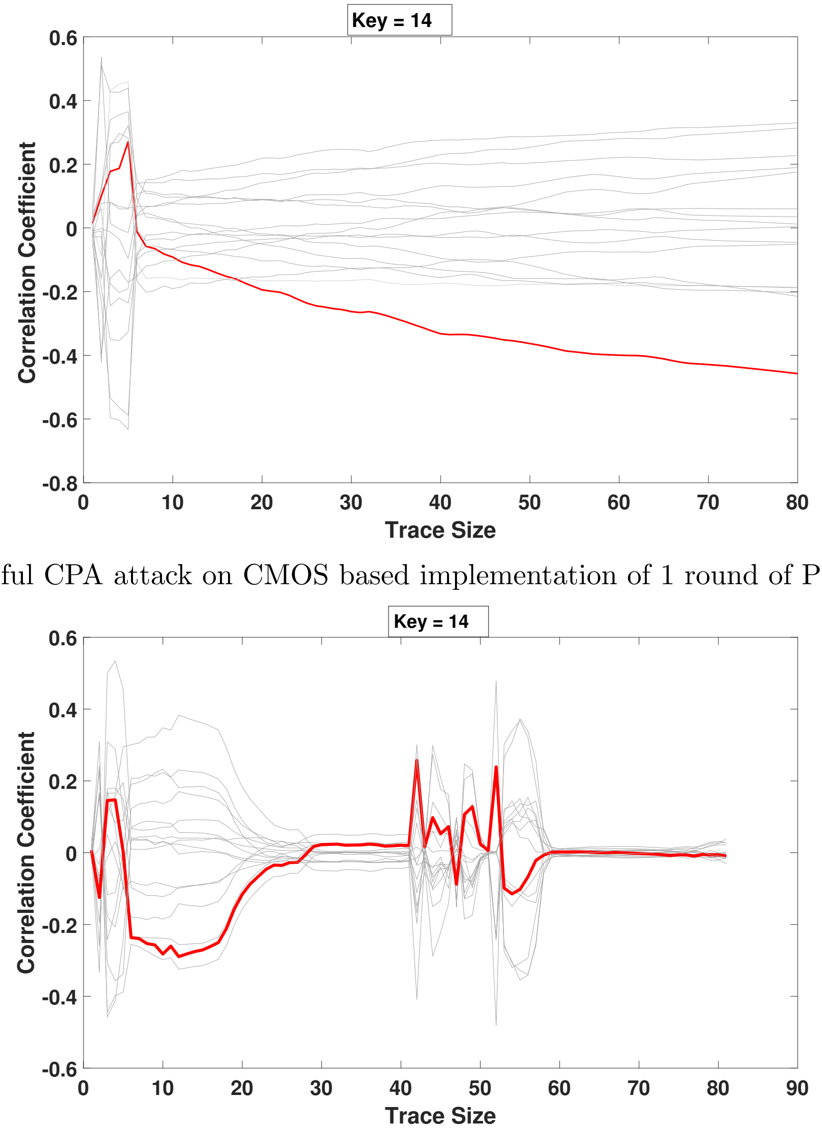
SPFAL implementation of PRESENT-80 as a function of frequency. From Figure 3.9 and Table 3.2 we can see that when using sinusoidal power clocks, 2-EE-SPFAL consumes less energy than its CMOS counterpart through 25MHz. We can see that at 12.5MHz, there is an average energy saving of 24.67% between CMOS and 2-EE-SPFAL-based designs. From 100 kHz to 25 MHz, our results show an average energy saving of 76.5% to 21.3% between CMOS and 2-EE-SPFAL with a clock generator implemented.

Table 3.2: Energy per cycle of one round of PRESENT-80 implemented with CMOS and 2-EE-SPFAL.

| Energy Per Cycle (pJ) | 100kHz | 500kHz | 1MHz | 5MHz | 10MHz | 12.5MHz | 25MHz |
|---|---|---|---|---|---|---|---|
| CMOS | 1.1 | 0.54 | 0.46 | 0.41 | 0.40 | 0.40 | 0.40 |
| 2-EE-SPFAL | 0.27 | 0.25 | 0.25 | 0.27 | 0.30 | 0.30 | 0.31 |

### 3.4.3 CPA Attack on PRESENT-80

2-EE-SPFAL-based implementation of PRESENT-80 has been shown to reduce energy when compared to CMOS. However, it is important to validate the security of 2-EE-SPFAL. The S-Box layer of PRESENT-80 is chosen as the attack point (Figure 3.7). The CPA attack is performed by following the steps described in [81]. The simulation was performed at 12.5MHz with a 100 fF load. The sinusoidal wave implementation of 2-EE-SPFAL was used as the test circuit. Practical CPA attacks usually



(a) Successful CPA attack on CMOS based implementation of 1 round of PRESENT-80.

(b) Unsuccessful CPA Attack on 2-EE-SPFAL based implementation of 1 round of PRESENT-80.

Figure 3.10: Correlation power analysis performed on both CMOS and 2-EE-SPFAL implementation of PRESENT-80 (© 2022 IEEE).

require greater than 100,000 traces to be successful. However, we are performing a simulation that is absent from electrical noise and therefore we require much fewer traces. We have chosen 80 samples per clock period thus we will sample every 1ns assuming a clock period of 80ns. 5120 input traces were necessary to complete a successful CPA attack on the CMOS-based design of PRESENT-80. Figure 3.10a shows a successful CPA attack on a CMOS implementation of PRESENT-80.

While the CMOS key was revealed in 5120 traces, the 2-EE-SPFAL implementation of PRESENT-80 did not reveal the key in greater than 12,000 traces. Figure 3.10b shows an unsuccessful CPA attack against the 2-EE-SPFAL implemented

PRESENT-80. This case study shows that 2-EE-SPFAL is a promising candidate for secure and low-energy smart electronic devices.

## 3.5 Conclusion

In this chapter, we have demonstrated the applicability of secure 2-phase adiabatic logic as a novel computing paradigm to design low-energy and secure smart electronic devices. One round of PRESENT-80 is designed using both standard CMOS and adiabatic design principles as a case study. The circuits were analyzed and simulated using Cadence Spectre. The results show significant energy savings between the adiabatic design and the CMOS design. Along with energy savings, the adiabatic implementation of PRESENT-80 was able to keep the key secret when a Correlation Power Analysis attack was performed on the circuit.

## Chapter 4

## Energy-Efficient Adiabatic Magnetic Tunnel Junction Logic for secure and low energy IoT devices

Dynamic and static power consumption are major sources of power within modern integrated circuits. Adiabatic logic is a design technique that can be used to reduce the dynamic power consumption of a circuit. To reduce the static power, we look to an emerging memory device known as Magnetic Tunnel Junctions (MTJs). MTJs can replace the standard Bulk-MOSFET and capacitive-based memories that leak substantial current. Thus, in this chapter, we introduce a Logic-in-Memory architecture that reduces dynamic power with adiabatic logic and static power with MTJs. The proposed Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML) is low energy and designed in such a way that it is CPA-resistant. The proposed implementation of PRESENT using EE-ACML reduces energy consumption between 66.99% and 86.58% at frequencies between 12.5MHz and 100MHz when compared with a CMOS/MTJ design proposed in the literature. Further, we demonstrate the resilience of the circuit against power analysis attacks by unsuccessfully stealing a secret key while performing a CPA attack.

The research work presented in this chapter was previously presented in [52] as Kahleifeh, Zachary, and Himanshu Thapliyal. "EE-ACML: Energy-Efficient Adiabatic CMOS/MTJ Logic for CPA-Resistant IoT Devices." Sensors 21.22 (2021): 7651. © 2021 MDPI and [51] as Kahleifeh, Zachary, and Himanshu Thapliyal. "Low-Energy and CPA-Resistant Adiabatic CMOS/MTJ Logic for IoT Devices." 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2021.

### 4.1 Proposed Energy-Efficient Adiabatic CMOS/ MTJ Logic (EE-ACML)

This section introduces the generic structure of our proposed Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML) and its operation. The proposed AND/NAND gate circuit can be seen in Figure 4.1. We can see that the structure consists of an adiabatic clock connected to a 2P2N Sense Amplifier. T1-T4 makes up the NMOS-only evaluation network connected to two MTJs (MTJ1 and MTJ2) with parallel and antiparallel configurations. Finally, transistors T5 and T6 are used to discharge any current stored in the load capacitors at the end of a clock cycle (When VPC is 0). A single EE-ACML gate requires two signals to operate correctly, a two-phase adiabatic clock and a discharge signal. When more than two gates are cascaded together, EE-ACML requires two sinusoidal clocks 180° out of phase as well as two discharge

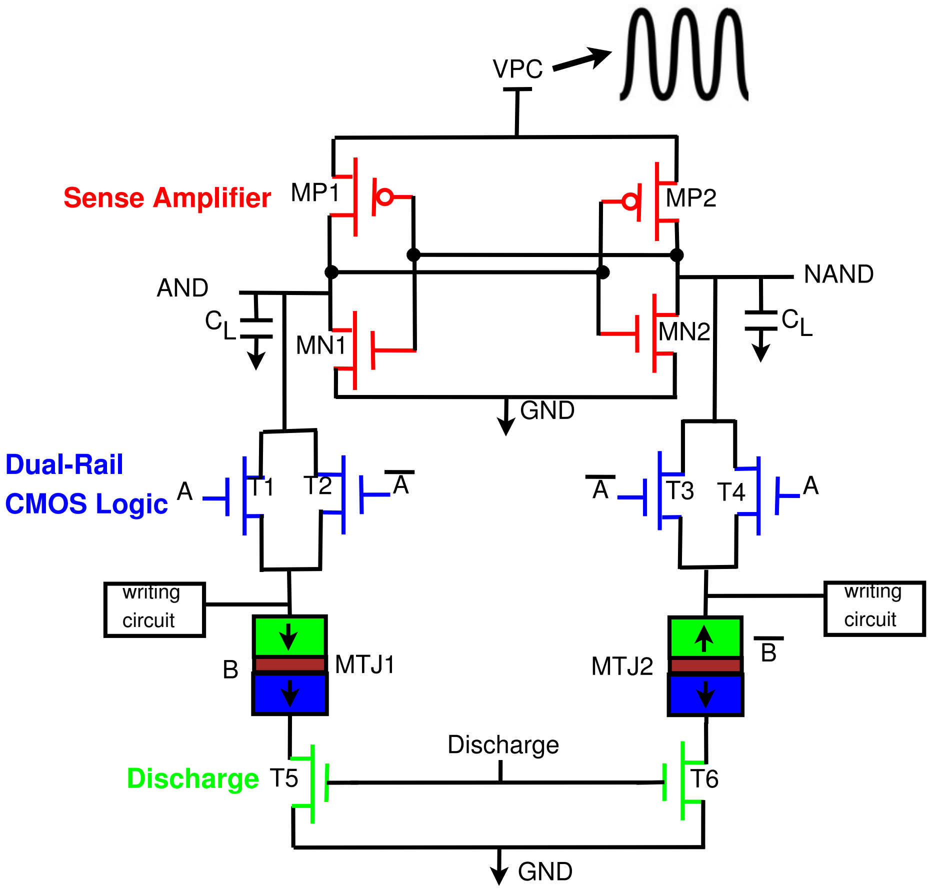


Figure 4.1: Proposed Energy-Efficient Adiabatic CMOS/MTJ AND/NAND gate.

signals in phase with the respective clocks. The complete adiabatic clocking waveform used to operate EE-ACML is shown in Figure 4.2.

### 4.1.1 Proposed adiabatic CMOS/MTJ operation

This section will explain the operation of EE-ACML. The operation will be explained with the AND/NAND gate seen in Figure 4.1.

#### Discharge stage

At the start, we will assume that A = 1, MTJ1/B = 1, discharge = 1, and VPC = 0. The operation is illustrated in Figure 4.3a. When the discharge signal is 1, T5 and T6 are on and thus MP2 is connected to ground through T1 and T5. When MP2 is on, AND follows VPC which is currently 0. When AND is at 0, MP1 is also turned on and thus NAND is also at 0.

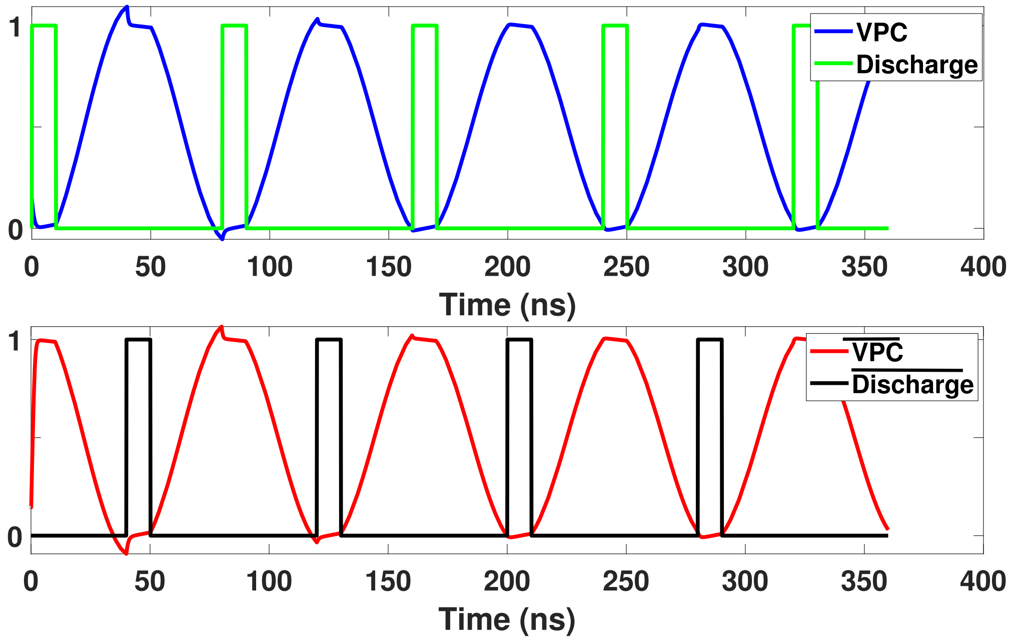


Figure 4.2: CPA-resistant two-phase adiabatic logic clocking scheme used in EE-ACML [7].

### Evaluate Phase

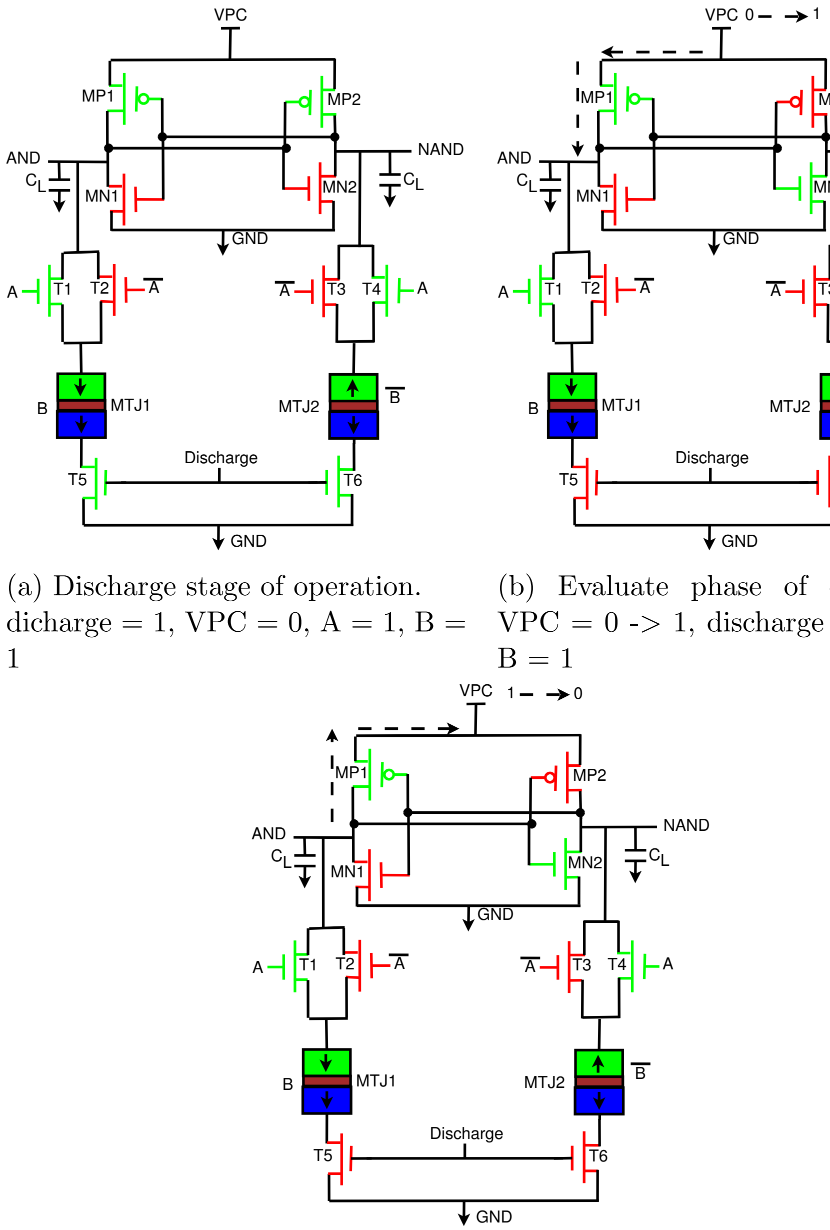
In this phase, the inputs remain at their current values. Discharge is now 0 and VPC begins to rise from 0 to 1. The operation of this stage is illustrated in Figure 4.3b. AND and NAND both rise with VPC, however, due to the difference in resistance between MTJ1 and MTJ2, one path will conduct more current. In this case, MTJ1 has lower resistance, and thus more current will flow through MP1. This will cause MP2 to turn off and MN2 to turn on. AND will rise with VPC to its peak value while NAND will pull down to logic 0 through MN2.

### Recover Phase

The operation of this stage is illustrated in Figure 4.3c. In this phase, VPC begins to drop from VDD to GND. At this point AND is at VDD and thus has a higher potential than VPC. Current will begin to travel from the high potential node to the low potential node at VPC. Charge is stored in the inductors and capacitors that make up the clock to be reused again in the next cycle and thus energy is recovered. At the end of the phase, the discharge signal will go to VDD to remove any remaining charge in the load capacitors.

### 4.1.2 Low Energy and Secure EE-ACML PRESENT Implementation

To show the energy efficiency and security of our proposed EE-ACML we will use the lightweight block cipher PRESENT as a case study [80]. Battery-operated IoT



(a) Discharge stage of operation. dicharge = 1, VPC = 0, A = 1, B = 1

(b) Evaluate phase of operation. VPC = 0 -> 1, discharge = 0, A = B = 1

(c) Recovery phase of operation. VPC = 1 -> 0, discharge = 0, A = B = 1

Figure 4.3: Operation of the proposed Energy-Efficient Adiabatic CMOS/MTJ AND/NAND.

devices have tight energy and area constraints thus the lightweight PRESENT is an ideal choice for these devices. In this chapter, we will demonstrate the energy efficiency and security of our proposed design using the 80-bit version of PRESENT. PRESENT has 31 rounds and consists of three stages: add round key, substitution layer, and a permutation layer. In this chapter, we will design 1 round to demonstrate energy efficiency and security.

### Substitution-Box

One of the components of PRESENT is the substitution box (S-box) which performs a non-linear substitution. When implemented with CMOS, the S-box is prone to Correlation Power Analysis Attacks (CPA). Thus, we look to implement the S-box with the proposed EE-ACML. In applications where data switches frequently the energy consumption of MTJ-based circuits is high as a result of the write energy [82]. With this in mind, we intend to design our S-box using a Look-Up-Table (LUT) based structure so we only have to write to the MTJs once. The structure of the proposed S-box is shown in Figure 4.4. The MTJs contain the outputs to the S-box which are constant and thus do not need to be switched [80].

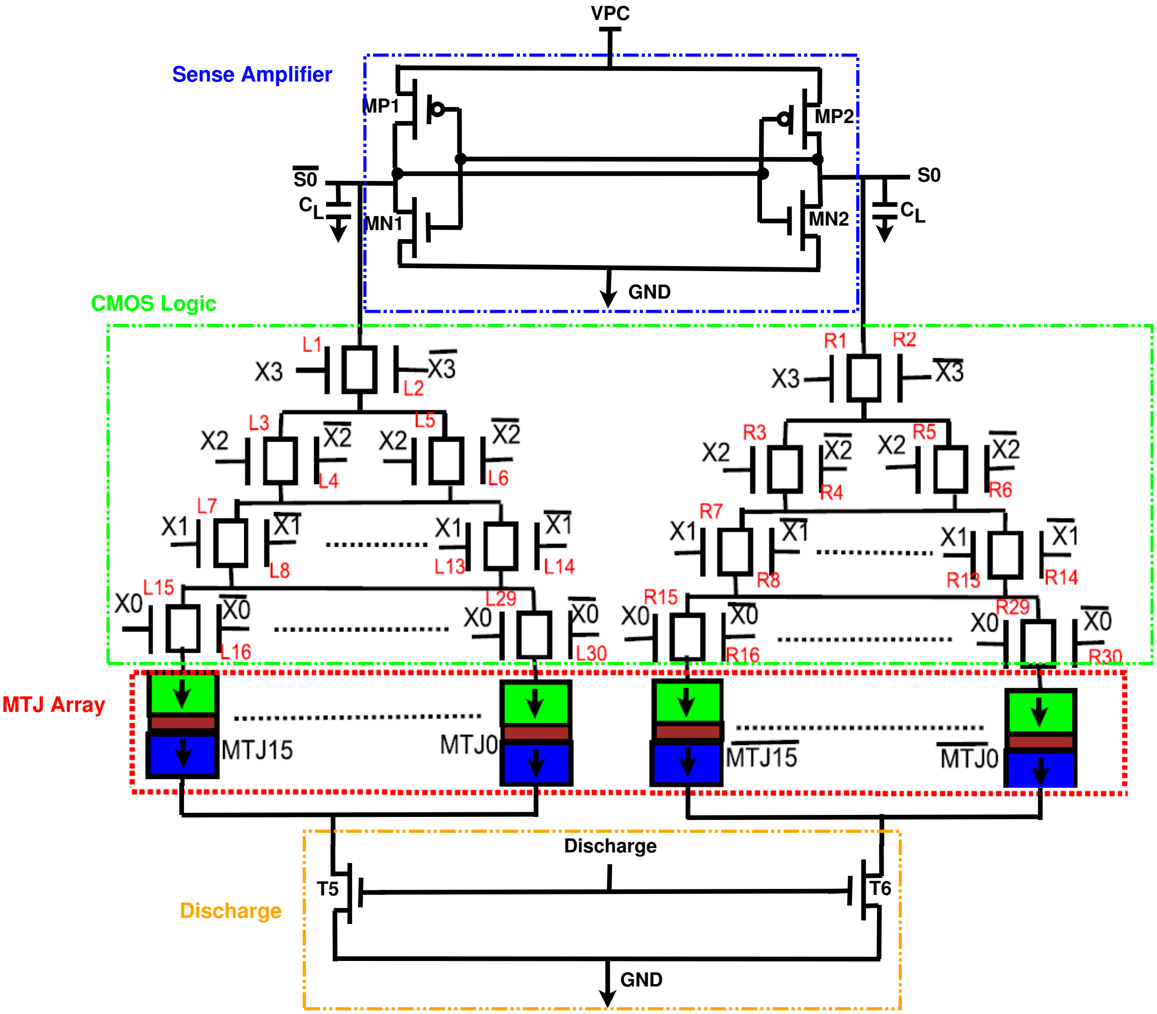


Figure 4.4: Proposed EE-ACML Look-Up-Table (LUT).

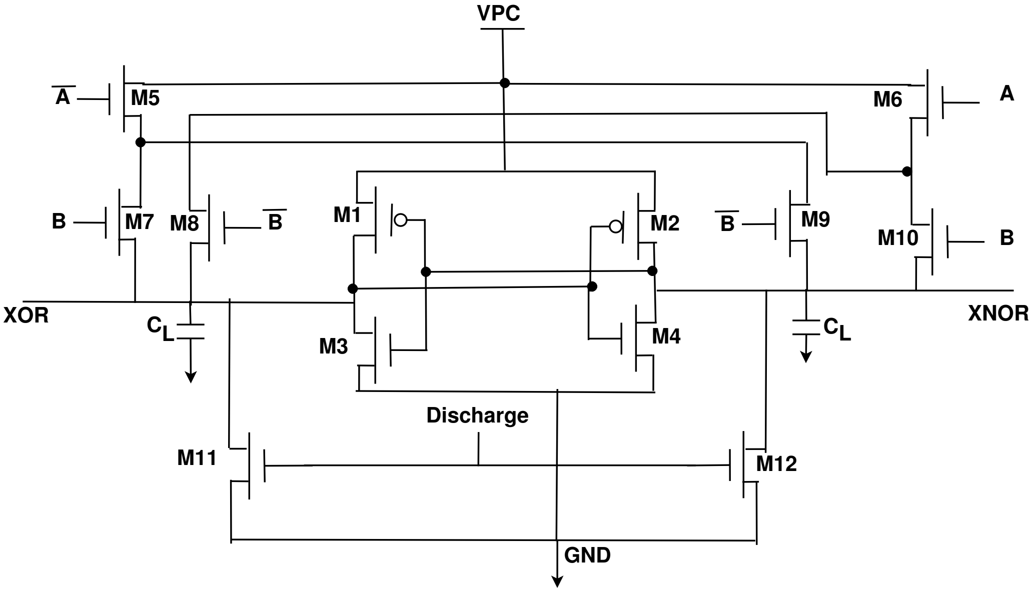


Figure 4.5: 2-EE-SPFAL XOR Gate used to implement the add round key stage of PRESENT [7].

### Add Round Key (XOR) Layer

Another component of PRESENT is the add round key layer which consists of an array of XOR gates. The CMOS/MTJ implementation of PRESENT utilizes a CMOS/MTJ-based XOR gate and thus cannot switch data often unless it pays a large energy penalty. In our implementation, we have designed our XOR gate using 2-EE-SPFAL [50]. 2-EE-SPFAL is a recently proposed two-phase CPA resistant adiabatic circuit. The two-phase clocking scheme allows for 2-EE-SPFAL to work in tandem with EE-ACML. Utilizing the 2-EE-SPFAL XOR gate means we can switch data frequently without having to worry about large energy consumption. The 2-EE-SPFAL XOR gate can be seen in Figure 4.5.

## 4.2 Results

This section presents the results of EE-ACML with the clock generator implemented. Simulations are performed using the Cadence Spectre simulator with 45nm standard CMOS technology. We have designed our circuits such that the MTJ switching is at a minimum thus we model our MTJs using a resistor. The resistance is determined by the models provided in [11] and the parameters shown in Table 4.1.

### 4.2.1 Analysis of Energy-Efficiency of the Proposed EE-ACML with Integrated Power Clock Generator

In this section, we examine the effect the adiabatic power clock generator has on EE-ACML. In our first study, we examine the effects of change in frequency and inductor

Table 4.1: Magnetic Tunnel Junction parameters used in simulations.

| Parameter | Description | Value |
|---|---|---|
| $t_{sl}$ | Thickness of free layer | 1.3nm |
| a | Length of surface long axis | 40nm |
| b | Width of surface short axis | 40nm |
| $t_{ox}$ | Thickness of the Oxide barrier | 0.85nm |
| TMR | 0.Tunnel Magneto Resistance ratio | 150% |
| RA | Resistance Area Product | $5\Omega\mu^2$ |
| Area | MTJ layout surface | 40nm x 40nm x $\pi/4$ |
| $R_p$ | Parallel resistance | 6.21 kΩ |
| $R_{ap}$ | Antiparallel resistance | 18.64 kΩ |

Table 4.2: One round of PRESENT inductor and capacitor values at various frequencies.

| Frequency | Capacitor (fF) | Inductor ($\mu$H) |
|---|---|---|
| 12.5M | 351.67 | 921.96 |
| 25M | 351.67 | 230.49 |
| 50M | 351.67 | 57.62 |
| 100M | 351.67 | 14.40 |

on energy per cycle. In this analysis, the capacitor is kept constant while the inductor is changed based on equation 4.1.

$$f = \frac{1}{2\pi\sqrt{L\frac{C}{2}}} \tag{4.1}$$

The capacitor and inductor values used in our simulations are shown in Table 4.2. The results of our analysis can be seen in Figure 4.6 and in Table 4.3. At 25 MHz and a capacitor and inductor value of 351.67 fF and 230.49 $\mu$H, our proposed circuit consumes 157.81 fJ/Cycle while the CMOS/MTJ implementation consumes 482.0 fJ/Cycle. This results in 67.25% energy savings between the two implementations of PRESENT. At 100 MHz and an inductor value of 14.40 $\mu$H, our proposed circuit consumes 459.56 fJ/Cycle which results in energy savings of 86.58%.

In our next study, we keep a constant frequency and vary the capacitor and inductor values to determine the effect on energy per cycle. Different values of inductors and capacitors result in varying power consumption of the RLC clock generator which can be seen in equation 4.2. Equation 4.2 gives the power consumption of a resonant RLC circuit in which L and $\omega_0$ vary with inductance and capacitance.

$$P_{avg} = \frac{V^2R\omega^2}{R^2\omega^2 + L^2(\omega^2 - \omega_0^2)^2} \tag{4.2}$$

Table 4.3: One round of PRESENT energy per cycle (fJ/Cycle) of EE-ACML and CMOS/MTJ [12]

| **Frequency** | **EE-ACML** | **CMOS/MTJ** [12] | **Energy Savings (%)** |
|---|---|---|---|
| 12.5M | 162.25 | 491.56 | 66.99 |
| 25M | 157.81 | 482.00 | 67.25 |
| 50M | 114.71 | 465.62 | 75.36 |
| 100M | 61.19 | 459.56 | 86.58 |

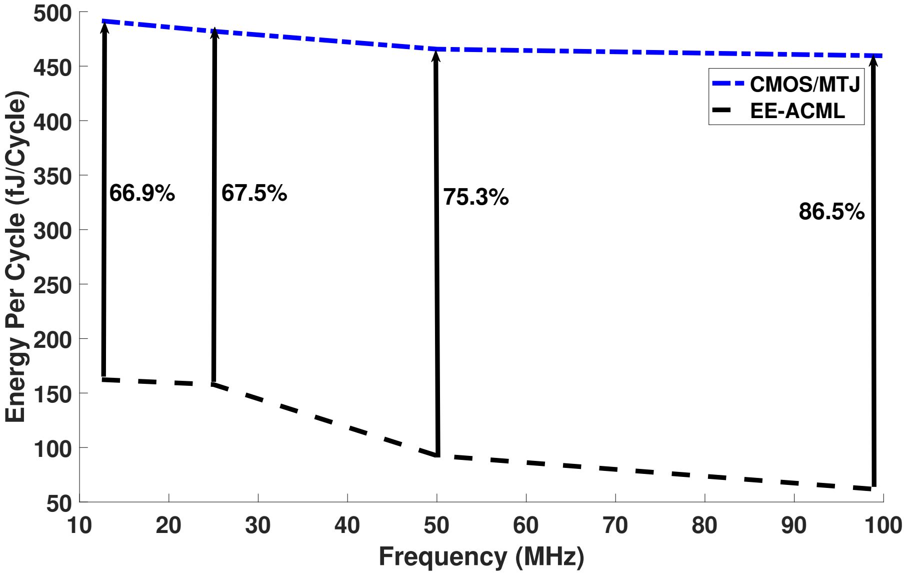


Figure 4.6: Energy per cycle comparison between proposed EE-ACML and CMOS/MTJ.

Thus, we theorize that the energy per cycle trend seen in Figure 4.7 is a result of the changing capacitors and inductors and thus the power of the RLC circuit.

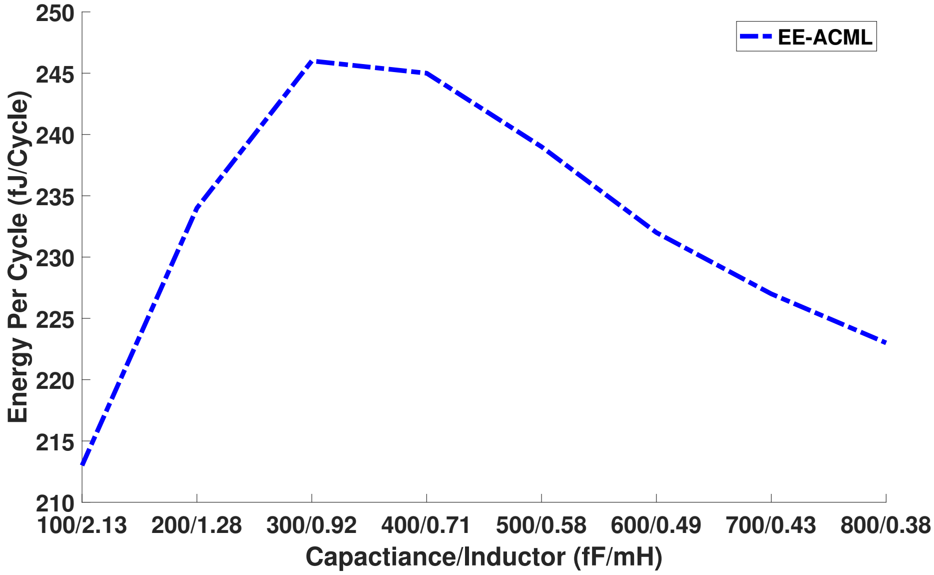


Figure 4.7: Effect of different inductor and capacitor values on energy consumption.

The adiabatic clock generator can also affect the security of our adiabatic CMOS/MTJ circuit. We vary the inductor and capacitor to determine the effect it has on Normalized Energy Deviation and Normalized Standard Deviation. The results can be seen in Figure 4.8. From Figure 4.8 we can see that the NED and NSD values peak at a certain inductor and capacitor values. We theorize that this is a result of the RLC power clock generator having higher power consumption at these inductor and capacitor values thus causing more variation in overall power consumption. We can conclude that there is a certain capacitor and inductor value that will result in a more robust countermeasure against CPA attacks.

### 4.2.2 Device Count of Proposed Energy-Efficient Adiabatic CMOS/MTJ Logic

The area consumption is an important metric when designing integrated circuits for IoT devices thus in this section we will present the device count of EE-ACML.

Table 4.4 shows the device count for various CMOS, CMOS/MTJ, and EE-ACML circuits. We can see that the EE-ACML AND/NAND gate has one less transistor than the CMOS/MTJ-based AND/NAND gate. The CMOS/MTJ substitution box has 4 extra transistors when compared to the EE-ACML substitution box.

We also recorded the number of transistors for one round of PRESENT. The CMOS/MTJ implementation of PRESENT has 4 fewer transistors than the EE-ACML implementation. This is because the CMOS/MTJ implementation uses the CMOS/MTJ XOR/XNOR gate while the EE-ACML implementation uses the 2-EE-SPFAL based XOR/XNOR gate which has more transistors. The trade-off of using

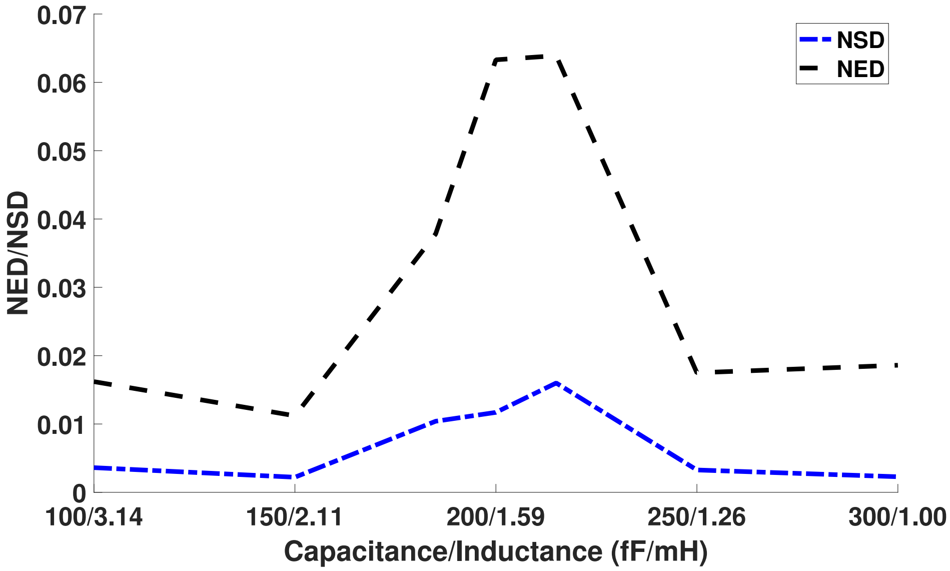


Figure 4.8: Effect of changing capacitor and inductor on NED and NSD.

the MTJ-based XOR/XNOR gate is it cannot be switched frequently without consuming substantial energy. EE-ACML uses fewer transistors than the CMOS implementation of PRESENT. This is because flip-flops are added to each CMOS output to synchronize the outputs.

### 4.2.3 Analysis of Security of the Proposed EE-ACML S-Box

In this chapter, we simulate and record the energy numbers of the PRESENT substitution box to calculate Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) values. Our simulations and results are with the adiabatic clock generator implemented. Table 4.5 shows the NED and NSD values for EE-ACML as well as a CMOS/MTJ S-box [12] and a purely adiabatic circuit 2-Energy Efficient-Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL)[7]. From Table 4.5 we can see that our proposed adiabatic CMOS/MTJ circuit consumes average energy of 41.6 fJ while the CMOS/MTJ implementation consumes 78.2 fJ and the 2-EE-SPFAL circuit consumes 35.2fJ at 12.5 MHz. Furthermore, our proposed S-box has a NED value of 0.0011 and an NSD value of 0.002, both lower than the CMOS/MTJ and 2-EE-SPFAL implementation of the PRESENT S-box.

## 4.3 Correlation Power Analysis Attack on EE-ACML Based PRESENT

In this section, we will demonstrate EE-ACML-based PRESENT resilience against a CPA attack. The adiabatic clock generator is implemented again to determine if the circuit remains secure. As the key is used for the operation of the substitution box, it will be used as the attack point. The CPA attack is performed by following the steps described in [81]. The simulation was performed at 12.5 MHz with a key

Table 4.4: Device counts of various CMOS, CMOS/MTJ, and EE-ACML based circuits.

| **Logic Family** | **Logic Gate** | **Transistor Count** |
|---|---|---|
| Proposed EE-ACML | NAND | 10 |
| | XOR | 10 |
| | SBOX | 264 |
| | 1-Round PRESENT | 4996 |
| CMOS/MTJ [12] | NAND | 11 |
| | XOR | 11 |
| | SBOX | 268 |
| | 1-Round PRESENT | 4992 |
| CMOS | NAND | 4 |
| | XOR | 8 |
| | SBOX | 216 |
| | 1-Round PRESENT | 5120 |

Table 4.5: Normalized Energy Deviation and Normalized Standard Deviation values for EE-ACML-based S-box.

| **Parameter** | **EE-ACML** | **CMOS/MTJ** [12] | **2-EE-SPFAL** [7] |
|---|---|---|---|
| $E_{min}(fJ)$ | 41.4 | 77.3 | 34.2 |
| $E_{max}(fJ)$ | 41.9 | 79.1 | 36.3 |
| $E_{avg}(fJ)$ | 41.6 | 78.2 | 35.2 |
| $NED$ | 0.011 | 0.022 | 0.056 |
| $NSD$ | 0.002 | 0.006 | 0.012 |

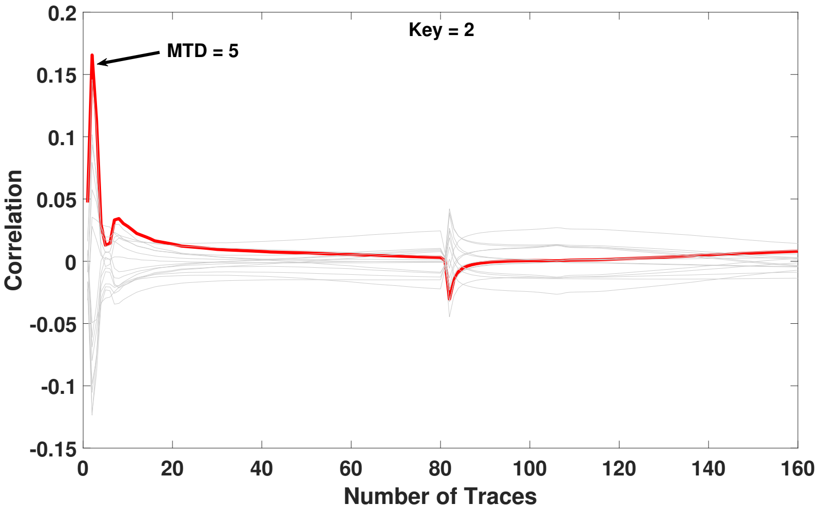
value of 2 $(0010)_b$. In the field, CPA attacks usually require hundreds of thousands of traces to steal encryption keys as a result of electrical noise and other non-ideal factors. However, in our simulations, we require fewer traces because the noise factors are not present. To demonstrate the ability of our CPA attack we have performed one on a CMOS-based PRESENT circuit and determined that the key can be stolen [51]. We will use the same CPA attack on the EE-ACML-based PRESENT to confirm the CPA-resistant ability of EE-ACML.

In our attack on the CMOS-based PRESENT, we utilized 160 traces and were able to steal the encryption key. Figure 4.9a shows a successful CPA attack against the CMOS implemented PRESENT S-box for a key value of 2. The Measurements to Disclosure (MTD) was 5 traces. In our attack on the EE-ACML-based PRESENT, we used 16000 traces and were unable to retrieve the key. Figure 4.9b shows an unsuccessful attack when the key value is 2 where the attack produced a guess of 1. The unsuccessful CPA attack on EE-ACML-based PRESENT shows it is a promising solution to defending against power analysis attacks on IoT devices.

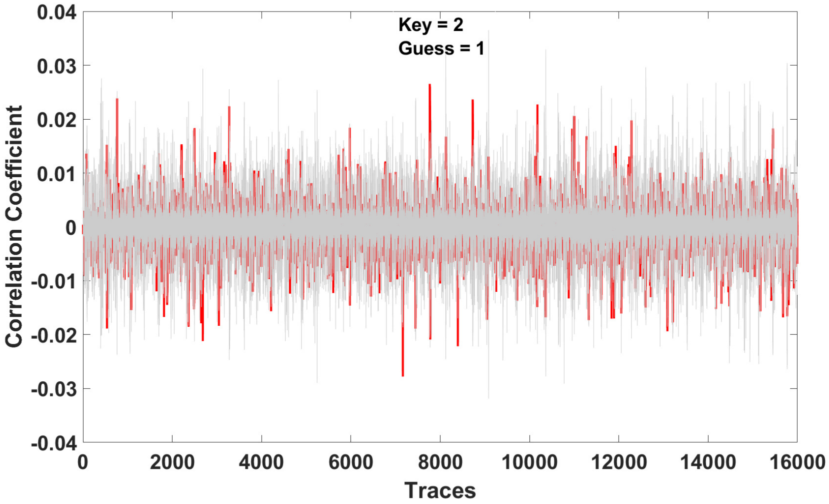
## 4.4 Summary

In this chapter, an adiabatic CMOS/MTJ architecture known as Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML) was presented and shown to be both energy efficient and secure. An adiabatic clock generator was implemented to show energy savings, security, and reliability remained. The novel circuit provides substantial energy savings when compared to a
CMOS/MTJ circuit found in the literature [12]. As a case study, we have constructed one round of PRESENT and shown our circuit remains energy efficient. Our circuit consumes 156.81 fJ/Cycle which amounts to 67.25% energy savings when compared to the CMOS/MTJ implementation. To demonstrate secure operation we have performed a Correlation Power Analysis attack on our EE-ACML-based PRESENT circuit and show that the keys remained secret.

Our work demonstrates the effectiveness of both adiabatic logic and magnetic tunnel junctions in designing low-energy and secure circuits. The low-energy consumption makes the novel circuits ideal candidates to be implemented within battery-constrained IoT devices. The implementation of an adiabatic clock generator also aids in proving our proposed circuits' ability to remain energy-efficient and secure. To further scrutinize the security of our device, machine learning-based CPA attacks can be performed on our design to determine the resilience [83]. Machine learning-based CPA attacks require fewer traces and higher test accuracy.



(a) Successful CPA attack on CMOS based implementation of PRESENT S-box with key = 2.



(b) Unsuccessful CPA attack on EE-ACML based implementation of PRESENT S-box with key = 2.

Figure 4.9: Correlation power analysis performed on EE-ACML implementation of PRESENT-80.

## Chapter 5

# Adiabatic/MTJ based Physically Unclonable Function for IoT Security

Physically Unclonable Functions (PUF) are useful security primitives in aiding defense against authentication, cloning, and key generation-based attacks. PUFs are circuits that utilize inherent process variation to generate a random but repeatable output. Here we define repeatable as the same PUF instance giving the same result given a challenge. Two different PUF instances should give different and hence, random values. In this chapter, we present a PUF based on both adiabatic logic and Magnetic Tunnel Junctions (MTJ). Adiabatic logic saves dynamic power consumption while MTJs offer a near-zero leakage power, non-volatile storage element with ample process variation for strong randomness. In this chapter, we also utilize our proposed PUF as a key generator for the PRESENT encryption circuit.

This work is currently under review in the IEEE Transactions on Consumer Electronics as Kahleifeh, Zachary, Himanshu Thapliyal, Syed M. Alam. "Adiabatic/MTJ based Physically Unclonable Function for Consumer Electronics Security." IEEE Transactions on Consumer Electronics.

## 5.1 Proposed Adiabatic/MTJ Physically Unclonable Function

Our proposed PUF utilizes both adiabatic logic and MTJs to generate energy-efficient and secure responses. The ramping effect of an adiabatic clock allows for energy recovery while the variation of the MTJs allows for randomness. MTJs have many sources of uncontrolled variation such as oxide thickness, free layer thickness, and the TMR ratio [84]. In our proposed PUF we intend to use these variations to generate strong responses.

Figure 5.1 shows the schematic representation of the proposed adiabatic/MTJ PUF. The proposed PUF contains the following components, an enable transistor, a sense amplifier, and two MTJs. The enable transistor is used to generate a response while the sense amplifier is used to sense differences in the resistances of the MTJs. The two MTJs are set in the same direction, either parallel or anti-parallel orientation when compared to the reference layer. As a result of process variation, one of these MTJs will have a higher resistance causing more current to flow through the other MTJ. It should be noted, that the sizing of the transistors should be increased to reduce process variation that occurs with transistors so that the response of the PUF is dominated by the variation of the MTJ [85].

It should be noted, that the proposed design will act as a dedicated security circuit

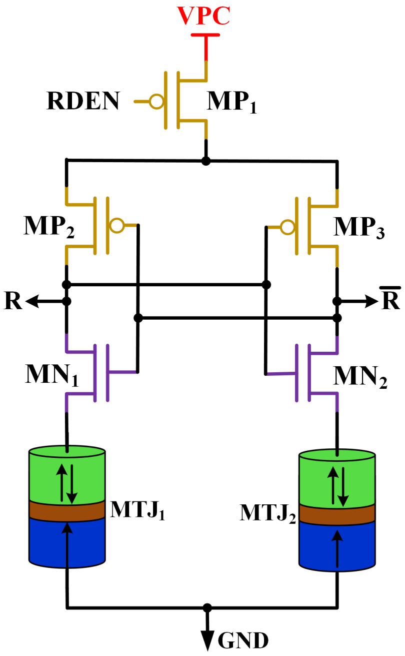


Figure 5.1: Proposed adiabatic/MTJ PUF. Proper connection to MTJ terminals avoids read disturbs.

rather than a memory circuit. In a typical memory operation, the two MTJs would need to be differential i.e two opposite orientations (P or AP). Further, the variation of the circuit needs to be as low as possible to reduce the Bit Error Rate (BER). To reduce the BER, the size of the MTJs and transistors are increased in-memory design. However, in our proposed design we do not need to increase the MTJ sizing as the variation of the MTJs is used to our advantage.

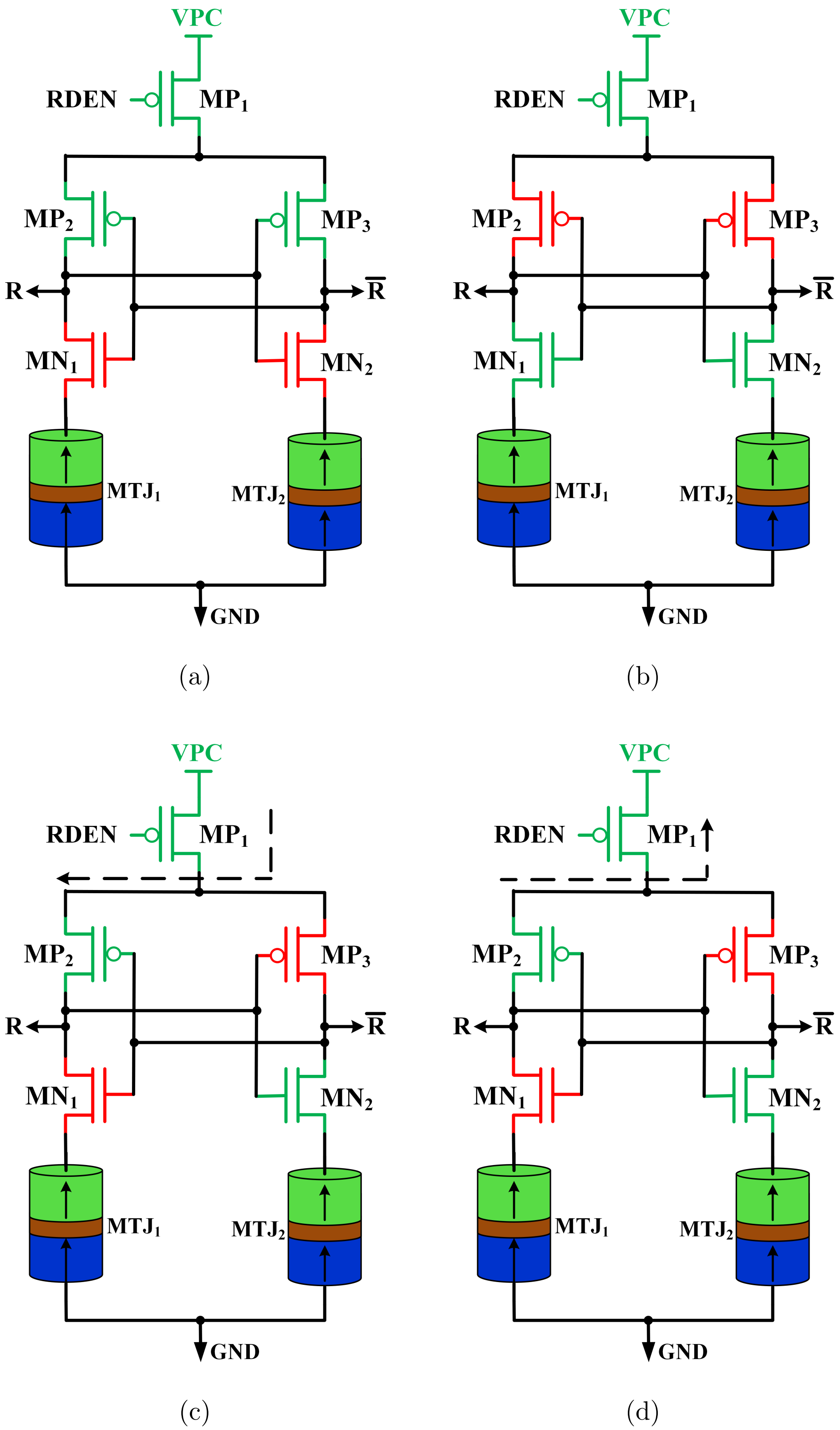
### 5.1.1 Operation of Proposed Adiabatic/MTJ PUF

In this section, we will go into greater detail on the operation of the proposed PUF. The proposed PUF operates using a two-phase adiabatic clock. The operation can be divided into two phases corresponding to the two phases of the clock, the evaluation phase and, the recovery phase.

#### Evaluate Phase

The first phase or the evaluate phase is where the PUF response is generated. In this phase, RDEN is set to 0 and VPC begins rising from GND to VDD. Both MTJ's are set to the same orientation, either parallel or anti-parallel. As a result of process variations, one MTJ will have a higher resistance than the other MTJ. MP2, MP3, MN1, and MN2 make up a sense amplifier that senses the difference in resistance and drives the outputs to either logic 0 or 1.

The operation of the proposed PUF is illustrated in Figure 5.2. In this example



(a)

(b)

(c)

(d)

Figure 5.2: Operation of proposed adiabatic/MTJ PUF including the evaluate and recovery phase.

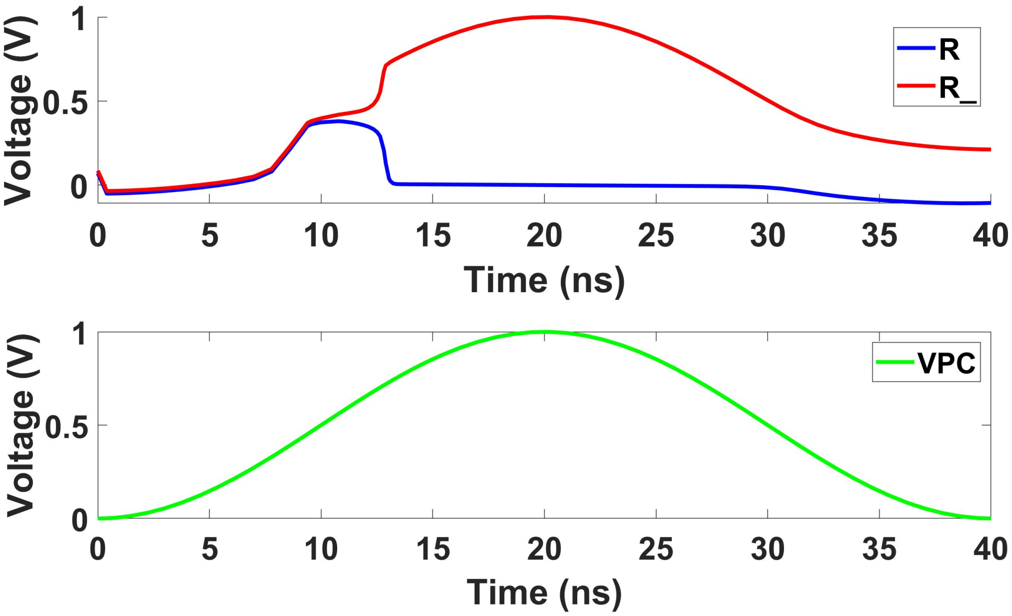
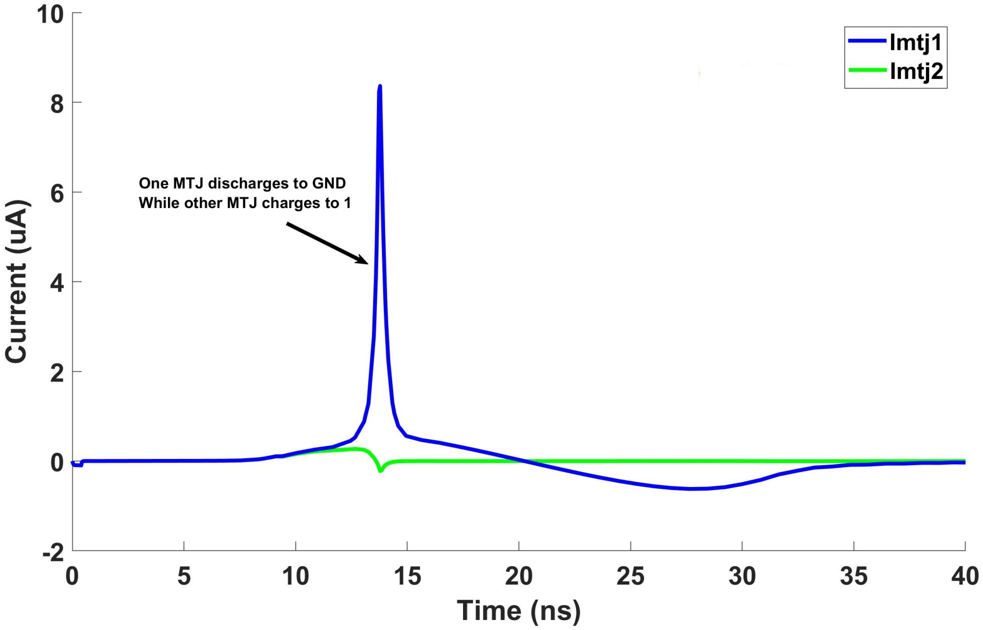


Figure 5.3: Output waveform of the proposed MTJ PUF.

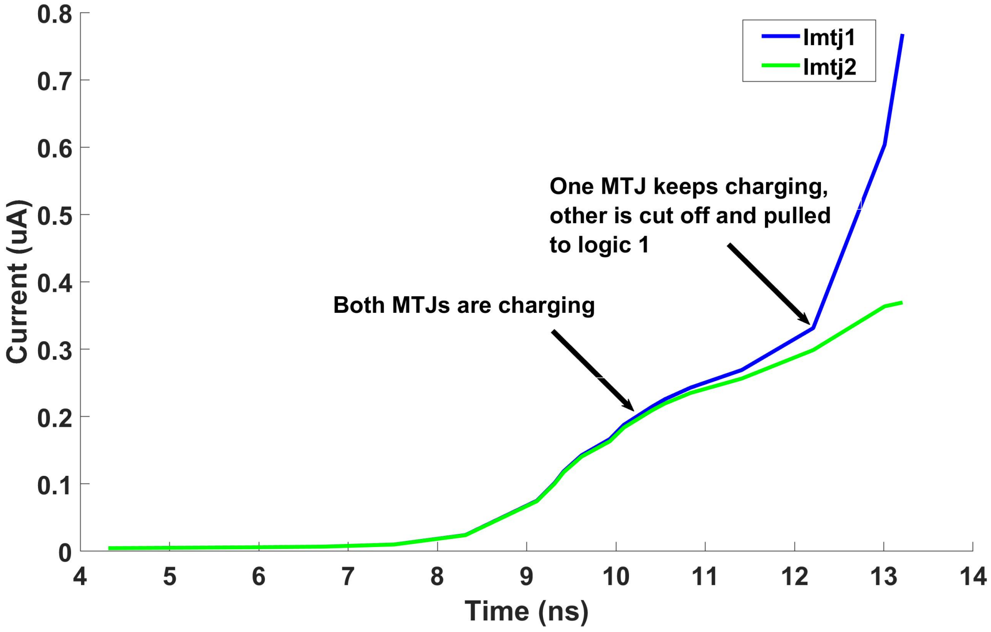
it is assumed that $R_{MTJ1} > R_{MTJ2}$ as a result of process variations. The operation begins with MP1, MP2, and MP3 conducting current and charging both outputs to $V_{tn}$ (Figure 5.2a). At this point, MN1 and MN2 are both conducting current through each respective MTJ (Figure 5.2b). As a result of MTJ1 having a higher resistance, more current is flowing through MTJ2 thus pulling $\overline{R}$ to ground and turning MP2 on. Output R is charged full VDD and output $\overline{R}$ is pulled to GND (Figure 5.2c). The output waveform for the response (R and $\overline{R}$) is shown in Figure 5.3. Both outputs charge until the variation of the MTJs dominate and force one output to logic 1 and the other output to logic 0. The operation is further exemplified in Figure 5.4. Figure 5.4a shows the current through each MTJ when a response is generated. As explained previously, one MTJ has higher resistance than the other which will force one output to charge to VDD and the other to be pulled to GND. Figure 5.4b shows a closer look at the current when the MTJ forces one of the outputs to charge to logic 1.

### Recover Phase

In the second phase or the recover phase, the clock begins to ramp down from VDD to GND. At this point, the output is at a higher potential than the clock thus current travels from high potential to low potential back into the adiabatic clock to be reused in the next cycle. The operation of the recovery phase is shown in Figure 5.2d as current is recovered through MP2 and MP1 back into the clock.



(a)



(b)

Figure 5.4: Current waveform for the proposed adiabatic/MTJ PUF. 5.4a shows the current across the entire response generation. 5.4b shows the current at the moment of switching.

## 5.2 Experimental Results

It is important to validate our proposed circuit to ensure energy efficiency and functionality. In this section, we present the simulation results of our proposed circuit. Simulations are performed using a Spice simulator with 45nm CMOS technology with perpendicular anisotropy CoFeB/MgO MTJ model [11]. Both MTJ orientations, parallel (P) and anti-parallel (AP) are taken into consideration when simulating and are both presented in the results.

Each bit of the response is from an individual PUF cell. One application of the proposed PUF is the generation of an encryption key thus in our simulations we have designed a 128-bit PUF array. In our simulations, we have chosen to run 200 Monte Carlo Simulations to mimic 200 unique integrated circuits.

### 5.2.1 Uniqueness Evaluation

Through simulations, we have determined that our proposed PUF has a uniqueness of 49.98% when the MTJ's are in a parallel orientation. While in the anti-parallel orientation our proposed PUF has a uniqueness of 49.99%. Regardless of orientation, the proposed PUF has very strong uniqueness values. A histogram of hamming distances between the 200 instances of the proposed 128-bit PUFs can be seen in Figure 5.5.

Furthermore, it is interesting to investigate whether the two orientations of the MTJ can result in two different PUF responses. Figure 5.6 shows a greyscale bitmap of the differences between the parallel and anti-parallel responses. Black boxes represent a location where the response bit is different. From Figure 5.6 we can see there are a large number of different response bits and thus we theorize that one PUF cell can produce two different responses.

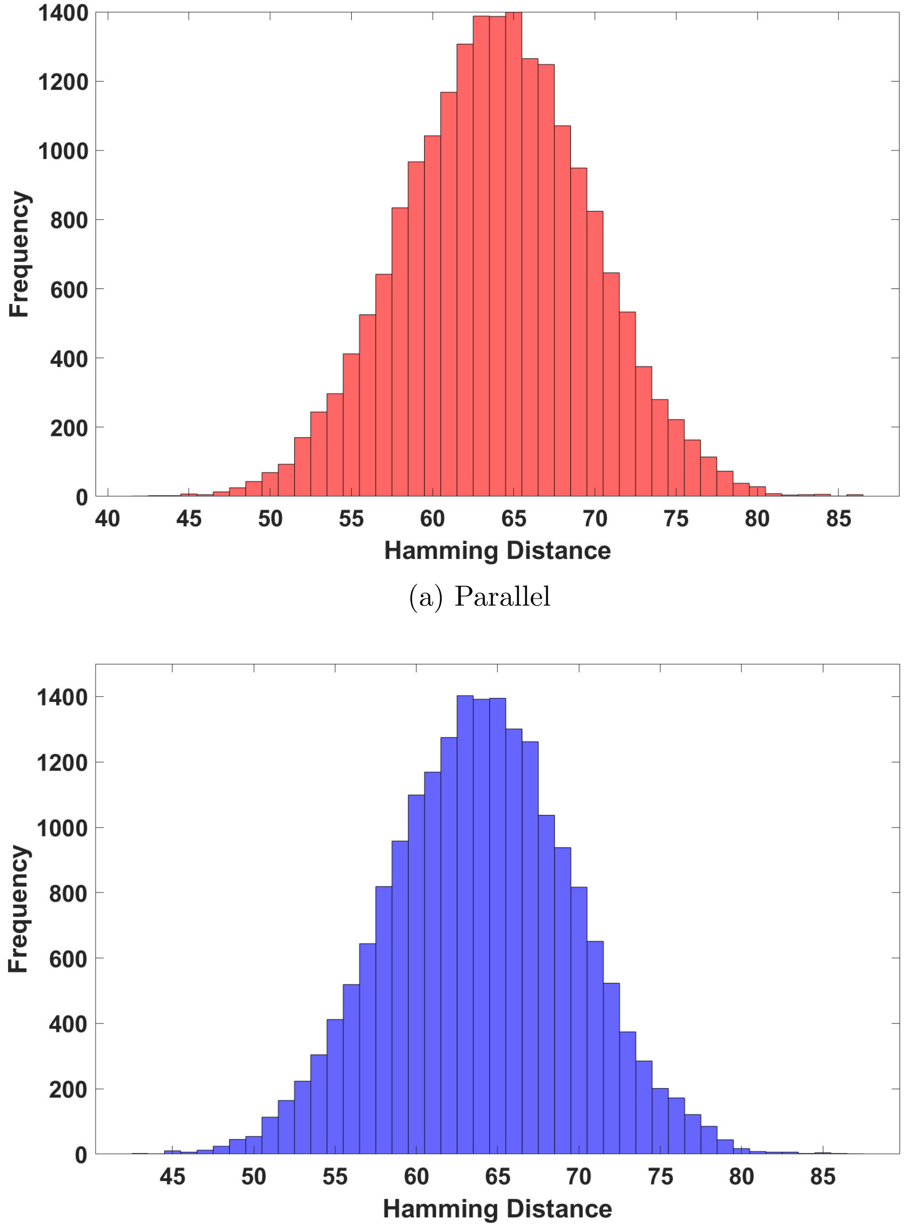
### 5.2.2 Uniformity Evaluation

The uniformity of our proposed adiabatic/MTJ PUF is 50.18% and 50.17% for the parallel and anti-parallel orientations, respectively. Both implementations are close to the ideal value of 50% implying that the proposed PUF response is difficult to predict. A greyscale bitmap of the two orientations is shown in Figure 5.7. Black boxes represent a "0" and white boxes represent a "1".

### 5.2.3 Reliability Evaluation

The average reliability of our proposed PUF across various temperatures, voltages, and TMR ratios is 97.07% and 96.97% for the parallel and anti-parallel orientations respectively. The worst-case reliability is 85.92% at a temperature of 100°C.

The reliability across various temperatures can be seen in Figure 5.8. Reliability values remain above 95% at temperatures between -40°C and 40°C. Between temperatures of 40°C and 100°C, the reliability of our proposed PUF drops to 85%. Whether our proposed PUF is in the P or AP mode has no strong correlation with the reliability. It should be noted that temperature has a strong effect on the reliability of



(a) Parallel

(b) Anti-parallel

Figure 5.5: Histogram of hamming distances between different PUF instances for both parallel and anti-parallel MTJ orientations.

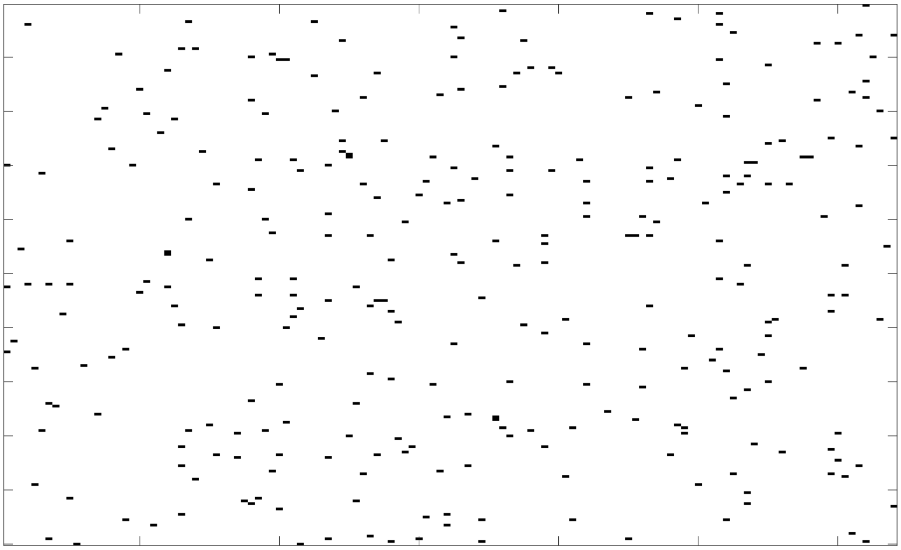


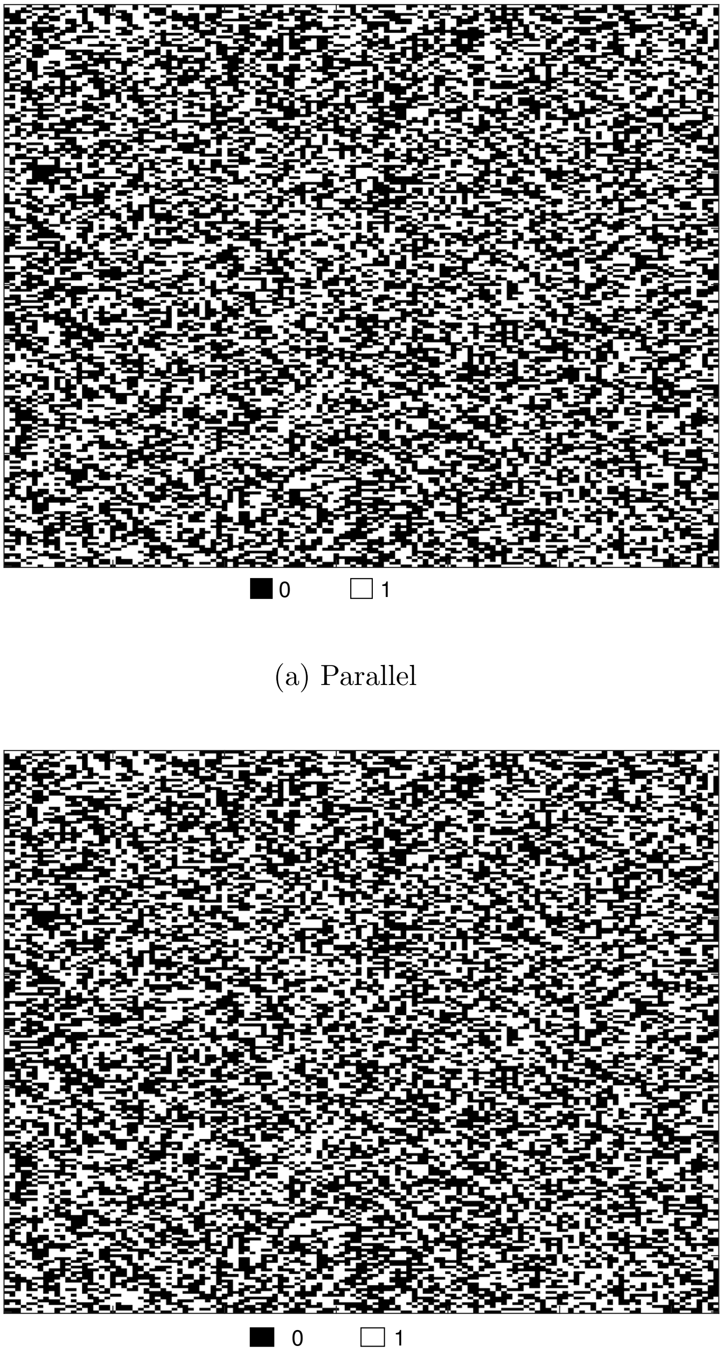
Figure 5.6: Difference in response between the parallel and anti-parallel orientation of the proposed adiabatic/MTJ PUF. Black boxes represent a flip in bits.

MTJ-based PUFs. To minimize the effects of temperature on reliability, Zhang et al. have proposed an automatic write-back feature to improve the reliability of MTJ-based PUFs [86]. The reliability of our proposed PUF across various voltages can be seen in Figure 5.9. The reliability of the proposed PUF remains above 99% for supply voltage values between 0.8V and 1.2V. At 0.8V, the reliability of the proposed PUF in parallel mode is 99.75% while in the anti-parallel mode has a reliability of 99.61%. At 1.2V, the reliability of the proposed PUF in parallel mode is 99.68% while in the anti-parallel mode has a reliability of 99.58%.

The reliability of our proposed PUF across various TMRs can be seen in Figure 5.10. The reliability of the proposed PUF remains above 99% for TMR values between 100 and 300 At a TMR of 100, the reliability of the proposed PUF in parallel mode is 99.72% while in the anti-parallel mode has a reliability of 99.27%. At a TMR of 300, the reliability of the proposed PUF in parallel mode is 99.30% while in the anti-parallel mode has a reliability of 99.72%.

## 5.3 Comparison with State-of-the-Art PUFs

In this section, we compare the energy consumption and security metrics of the proposed adiabatic/MTJ PUF with other state-of-the-art PUFs reported in the literature.



(a) Parallel

(b) Anti-parallel

Figure 5.7: Greyscale bitmap of the 200x128 proposed PUF for both parallel and anti-parallel orientations.

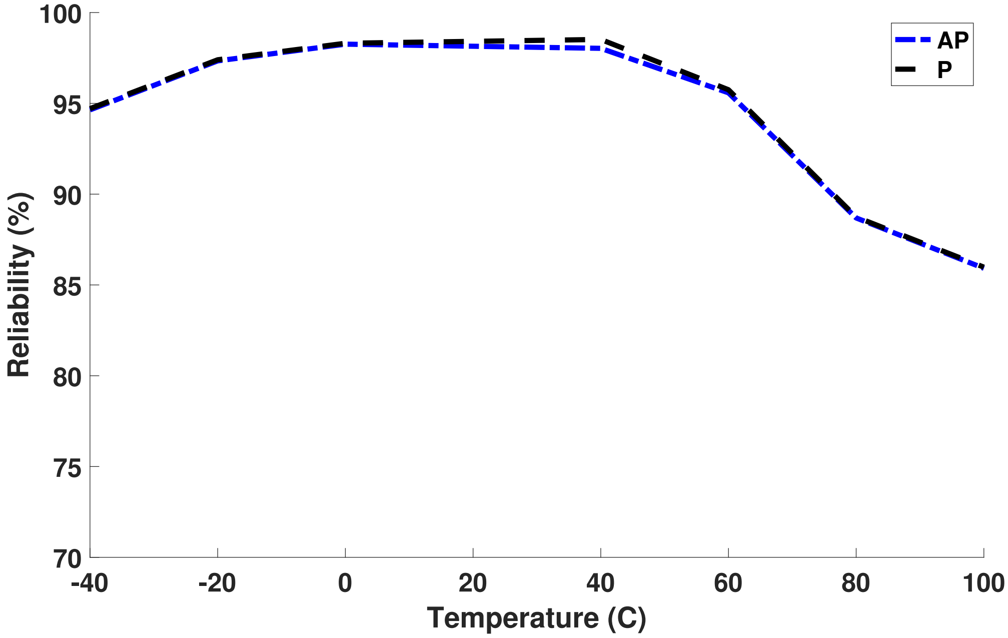


Figure 5.8: Reliability of proposed PUF across various temperatures.

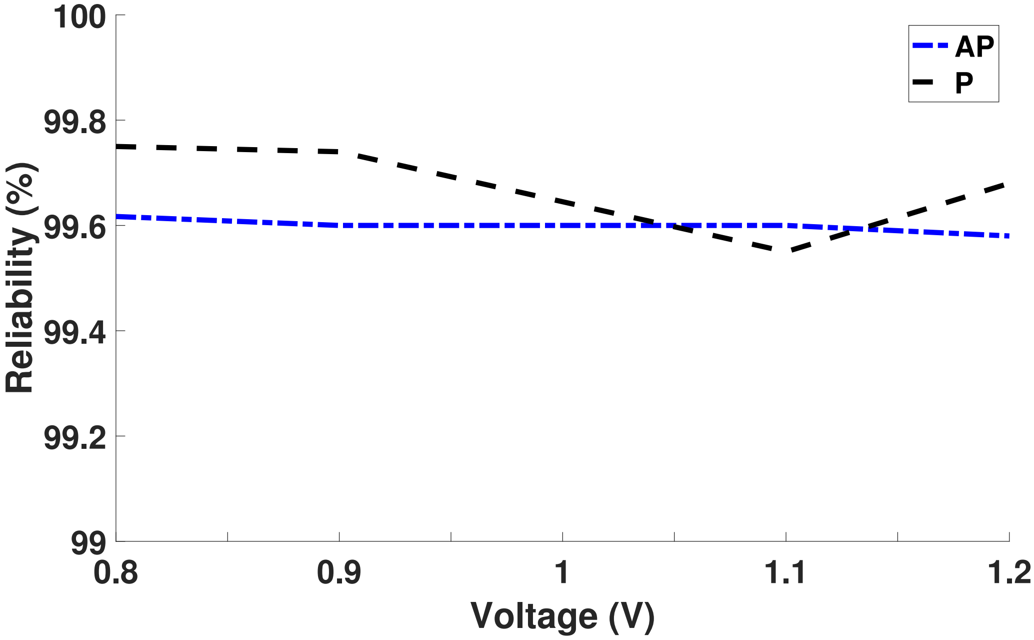


Figure 5.9: Reliability of proposed PUF across various supply voltage levels.

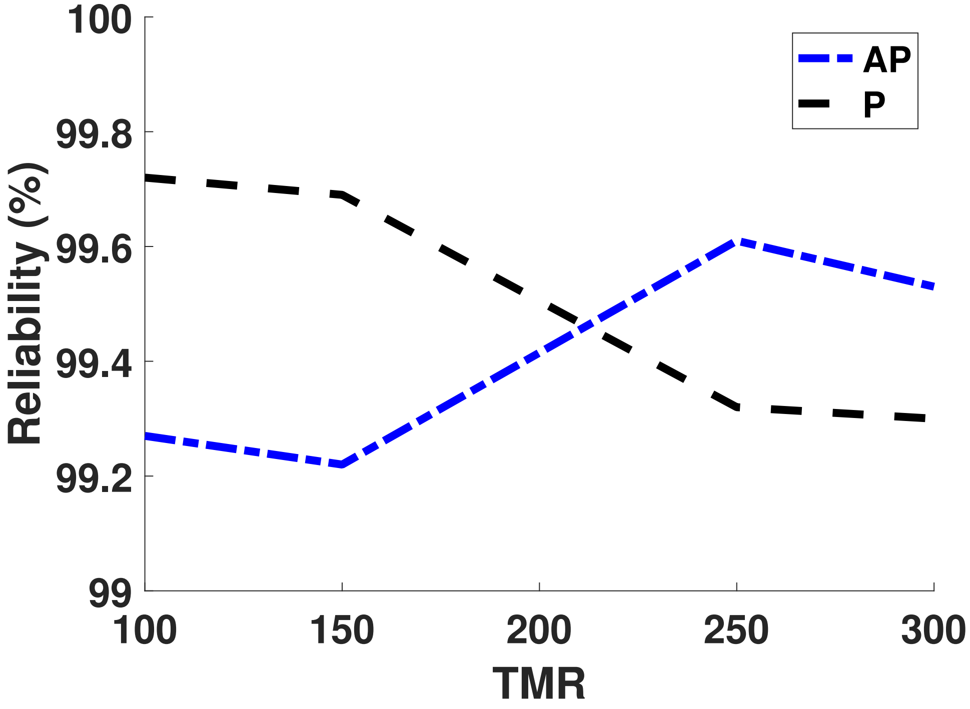


Figure 5.10: Reliability of proposed PUF across various TMR values.

Table 5.1: Energy consumption of proposed adiabatic/MTJ PUF compared with select PUFs from the literature.

| PUF | Tech. | VDD | Energy/bit |
|---|---|---|---|
| Lim et. al (2005) [87] | 180nm | 1.8V | 1.37pJ |
| Stanzione et. al (2011) [88] | 90nm | 1.2V | 3.8pJ |
| Majzoobi et. al (2011)[89] | 90nm | 1.2V | 15fJ |
| Cao et. al (2015)[90] | 180nm | 3.3V | 23.9pJ |
| Yang et. al (2015)[91] | 40nm | 0.9V | 17.75pJ |
| Neale et. al (2015)[92] | 28nm | 0.6V | 0.045fJ |
| Tao et. al (2016)[93] | 65nm | 0.6V | 10.3fJ |
| Zhang et. al (2015)[94] | 45nm/MTJ | 1V | 1.00fJ |
| Proposed (P) | 45nm/MTJ | 1.0V | 5.2fJ |
| Proposed (AP) | 45nm/MTJ | 1.0V | 5.1fJ |

### 5.3.1 Energy Consumption Comparison

The energy consumption of consumer electronic devices is an important metric, especially when considering battery-operated devices. Table 5.1 shows the energy per bit of the proposed adiabatic/MTJ PUF and other state-of-the-art PUFs. Our proposed adiabatic/MTJ PUF consumes 5.2fJ and 5.1fJ per bit in the parallel and anti-parallel orientations, respectively. From table 5.1, it can be seen that the proposed PUF has lower energy consumption compared with the other PUFs. It should be noted that [92] reports lower energy consumption than the proposed PUF, however, their design is at a lower technology node and supply voltage. Further, we compared with another CMOS/MTJ-based PUF [94] that reports an energy consumption of 1.00fJ per bit, the MTJ model used in this PUF has substantially lower resistance values and thus lower energy consumption.

### 5.3.2 Security Metric Comparison with State of the Art PUFs

Table 5.2 summarizes the comparison of results that are obtained verbatim from the respective papers. When compared with other CMOS/MTJ designs our proposed adiabatic/MTJ design has slightly better reliability values. The uniqueness value of the proposed adiabatic/PUF is closer to the ideal value of 50% when compared with the purely CMOS-based PUFs. The CMOS/MTJ PUF in [94] has a comparable uniqueness value to the proposed PUF. The uniformity of the proposed adiabatic/MTJ PUF is comparable with the CMOS-based designs as the best case uniformity is 0.04% away from the ideal value while our proposed PUF uniformity is 0.17% and 0.18% away from the ideal value. When compared with another 45nm/CMOS-based PUF our proposed PUF has lower energy consumption making it an ideal candidate for battery-constrained designs.

Table 5.2: Security metrics and energy consumption of proposed adiabatic/MTJ PUF compared with state of the art PUFs.

| PUF | Tech. | VDD | Key Size | Uniqueness | Uniformity | Reliability | Energy/bit |
|---|---|---|---|---|---|---|---|
| [87] | 180nm | 1.8V | 64 | NA | NA | 95.18% | 1.37pJ |
| [88] | 90nm | 1.2V | 256 | NA | NA | 99.9% | 3.8pJ |
| [89] | 90nm | 1.2V | 64 | NA | NA | 97% | 15fJ |
| [90] | 180nm | 3.3V | 64 | 49.37% | NA | 99.1% | 23.9pJ |
| [91] | 40nm | 0.9V | 256 | 47.22% | NA | $\geq$ 99.9% | 17.75pJ |
| [92] | 28nm | 0.6V | 128 | 49.11% | 49.96% | 88.39% | 0.045fJ |
| [93] | 65nm | 0.6V | 128 | 50.04% | 49.95% | 98.56% | 10.3fJ |
| [95] | 45nm | 1V | 128 | 49.48% | 49.41% | 99.60% | 0.08fJ |
| [94] | 45nm/MTJ | 1V | 128 | 51.01%/49.89% | 50.20%/49.90% | 96% | 1.00fJ |
| [96] | 40nm/MTJ | 1V | 128 | 49%-51% | 49%-51% | 96.73% | NA |
| Proposed (P) | 45nm/MTJ | 1.0V | 128 | 49.98% | 50.18% | 97.07% | 5.2fJ |
| Proposed (AP) | 45nm/MTJ | 1.0V | 128 | 49.99% | 50.17% | 96.97% | 5.1fJ |

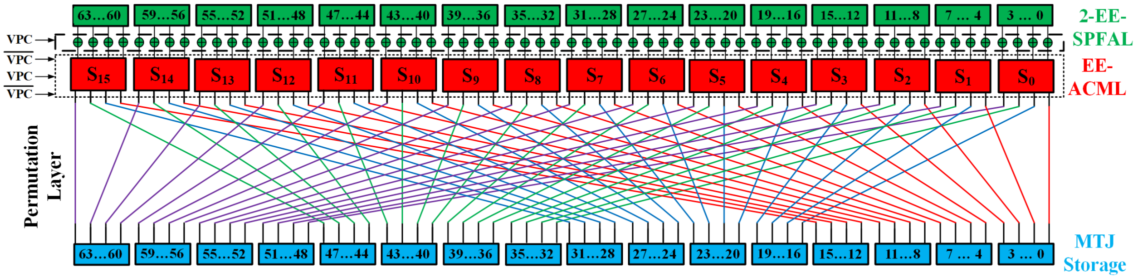


Figure 5.11: Structure of PRESENT implemented with adiabatic logic and adiabatic/MTJ logic.

## 5.4 Application of Proposed Adiabatic/MTJ PUF

One application of PUFs is the key generation of encryption circuits [47]. In this section, we demonstrate the applicability of our proposed adiabatic/MTJ PUF with the key generation of the PRESENT encryption standard [80]. Suh et al. suggest that when using a PUF for key generation, Error Correcting Codes (ECC) should be used to ensure the correct output is produced [47]. However, in our study, we ignore the ECC circuitry as our simulations are conducted without noise and in ideal conditions. Furthermore, if the encryption standard used requires the key to have a certain set of characteristics such as RSA, the PUF response can be used as a seed in a key generation algorithm. In our case, PRESENT only requires the key to be a random value thus we do not need to utilize any key generation algorithms.

The key generated from our proposed adiabatic/MTJ was used as the key to PRESENT encryption [80]. PRESENT is a lightweight block cipher with key sizes of 80-bits or 128-bits. In this article, we implement one round of the 80-bit version of PRESENT encryption. PRESENT consists of three stages: add round key, substitution, and permutation, the three stages can be seen in Figure 5.11. The implementation of PRESENT in this case study is based on that of a previous adiabatic/MTJ implementation of PRESENT. The add round key stage is implemented with a two-phase adiabatic XOR gate. The substitution layer is implemented using a hybrid adiabatic/MTJ look-up-table which is illustrated in Figure 5.12. The look-up table-based implementation is to ensure minimal switching of the MTJs. The implementation of the adiabatic/MTJ PUF within the PRESENT encryption is shown in Figure 5.13.

The proposed implementation of PRESENT with the key generating circuit was simulated through spice simulations to verify functionality and determine the energy consumption. Table 5.3 presents the energy consumption of the proposed design. At 12.5MHz, our proposed implementation of PRESENT consumes 0.52pJ per cycle. At 200MHz, our proposed design consumes 0.13pJ per cycle. We refrain from adding a comparative study with the CMOS-based counterpart because the random nature of key generation will result in different energy consumption. However, the various portions of the proposed PRESENT implementation have been shown to be energy efficient when compared with CMOS. Thus, we claim that the sum of parts will also

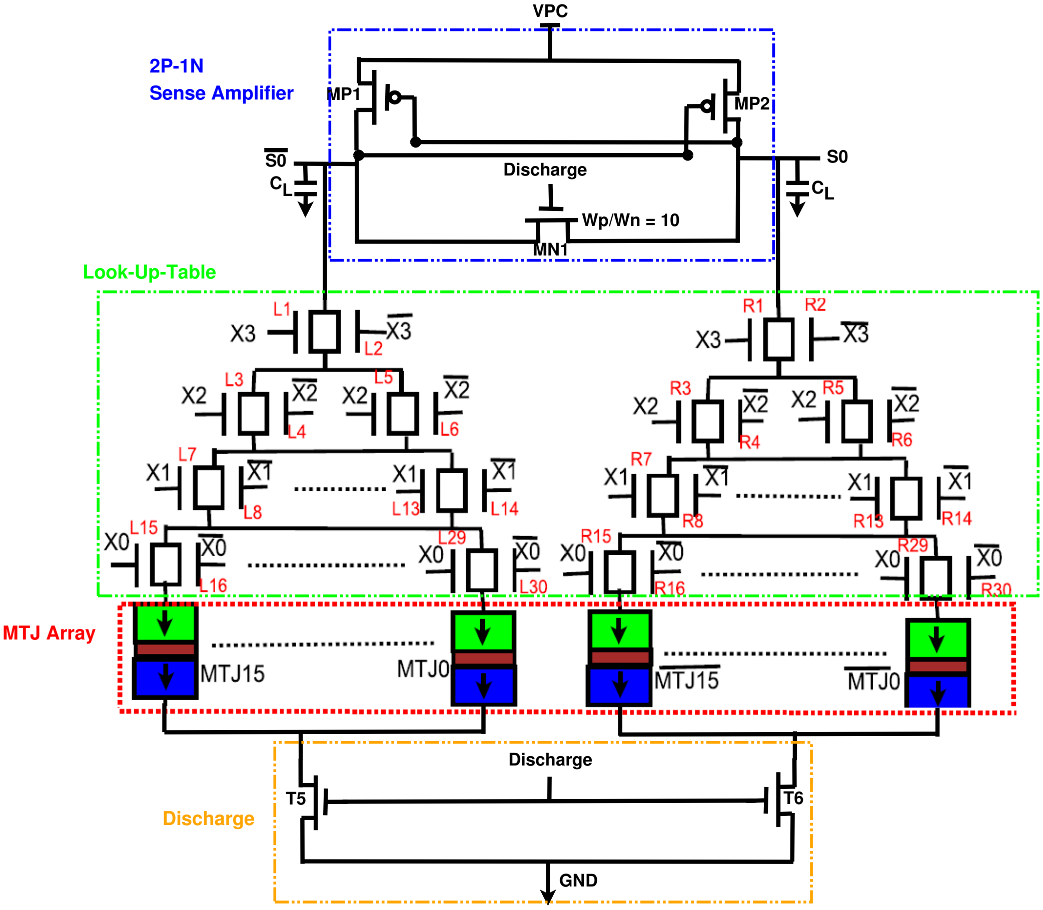


Figure 5.12: Adiabatic/MTJ Look-up-Table implementation of the substitution layer of PRESENT.

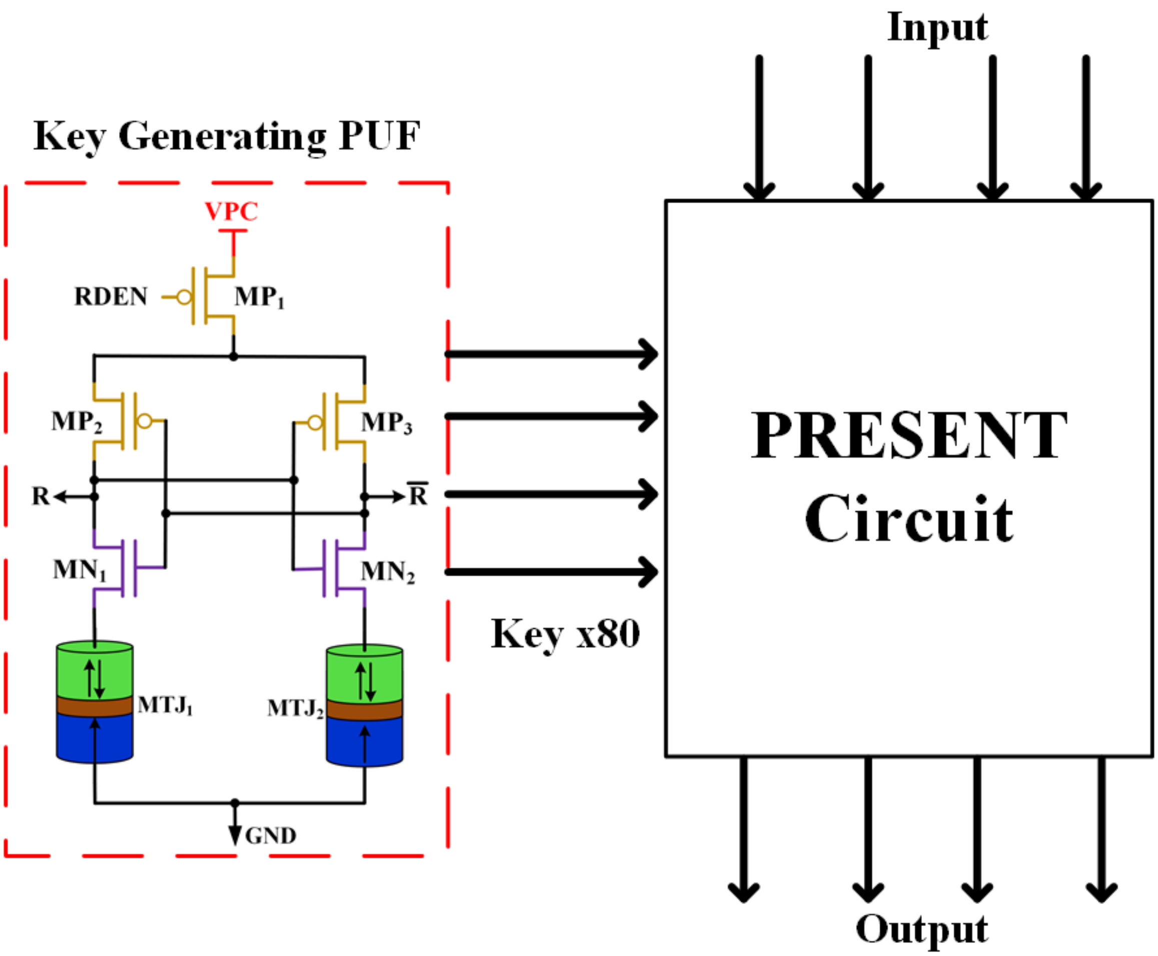


Figure 5.13: Implementation of proposed adiabatic/MTJ PUF in PRESENT key generation.

Table 5.3: Energy consumption of proposed PRESENT-80 with key generation PUF circuit.

| **Parameter** | **12.5MHz** | **25MHz** | **50MHz** | **100MHz** | **200MHz** |
|---|---|---|---|---|---|
| Energy per Cycle (pJ) | 0.52 | 0.43 | 0.22 | 0.20 | 0.13 |

be energy efficient when compared with CMOS.

## 5.5 Conclusion

In this chapter, we have presented a low energy and secure adiabatic/MTJ based-PUF. A two-phase adiabatic clock is used to reduce the dynamic energy consumption while the MTJ is used to generate the response bits. MTJs can either be in a parallel or anti-parallel orientation when referenced with the fixed layer. We investigate both orientations to determine the uniformity, uniqueness, reliability, and energy efficiency of the proposed adiabatic/MTJ PUF. We have determined that our proposed PUF is energy-efficient when compared to many CMOS and CMOS/MTJ-based PUFs. Low energy consumption and ideal uniqueness and uniformity values make our proposed adiabatic/MTJ PUF an ideal candidate for energy-constrained devices. The proposed PUF can be implemented in encryption key generation algorithms, device fingerprinting for intellectual property protection and device authentication, etc.

# Chapter 6

# Analysis of Adiabatic Clock Generators

The adiabatic clock generator is the driving force behind adiabatic circuits and is thus an important aspect when designing adiabatic systems. The common implementation practice for adiabatic clock generators is the use of inductors and capacitors to form an RLC generator. Adiabatic circuits can be constructed with a different number of phases such as two and four-phase. In the current literature, there is a lack of comparison on both the energy and security characteristics of two and four-phase clock generators. Thus, in this chapter, we compare the two and four-phase adiabatic clock generators in terms of energy efficiency and security against power analysis attacks. The security and energy consumption is evaluated in various conditions to mimic the practical conditions adiabatic circuits may operate in.

## 6.1 Simulation Results

This section presents simulation results for both two and four-phase adiabatic clock generators.

### 6.1.1 Energy Consumption of Adiabatic Clock Generators

Adiabatic circuits reduce the dynamic energy consumption of circuits through the use of time-varying power clocks. Adiabatic circuits recycle energy stored in load capacitors back into the clock generators to be reused again. Energy-efficiency of an adiabatic circuit is an important metric when considering whether it applies to low-power IoT devices. The clock generator circuity and inductors and capacitors that make up the generator can consume substantial energy. Thus, it is important to verify that adiabatic circuits remain energy-efficient when the clock generator is implemented. In chapters 3 and chapter 4, we demonstrate that our proposed adiabatic circuits remain energy-efficient with the addition of clock generators. However, we have neglected to compare the energy of two and four-phase adiabatic clock generators. Thus, in this section, we present our results on the energy consumption of both two and four-phase adiabatic clock generators when they are implemented in adiabatic circuits.

Table 6.1: Inductor values used in two and four-phase clock generators when powering PRESENT S-Box.

| Frequency (MHz) | Two-phase Inductance | Four-phase Inductance |
|---|---|---|
| 12.5 | 9.96mH | 377.2$\mu$H |
| 25 | 2.49mH | 94.32$\mu$H |
| 50 | 624.8$\mu$H | 23.58$\mu$H |
| 100 | 156.2$\mu$H | 5.89$\mu$H |
| 200 | 39.05$\mu$H | 1.47$\mu$H |

### Energy Consumption of Logic Gates

We first present a comparison of the energy consumption of various logic gates. It is important to compare the energy consumption of the basic logic gates in various non-ideal conditions as adiabatic circuits implemented within IoT devices will also be operating in non-ideal conditions. Thus, we compare the energy of two and four-phase clock generators while varying frequency, temperature, and load.

We first begin by examining the effects of frequency on the energy efficiency of adiabatic clock generators. We utilize the PRESENT S-box as a case study to observe these effects. When varying frequencies, the inductor and capacitor values should be adjusted to match the resonant frequency as explained in chapter 2. The load of the adiabatic circuit is used as the capacitance for the clock generator and is thus fixed at 26.8fF and 32.4fF for the four and two-phase clock generators, respectively. The inductor values are varied with frequency and are shown in Table 6.1.

The frequency effects on energy consumption can be seen in Figure 6.1. It can be seen that energy consumption increases as frequency increases which is expected as the adiabatic circuit's energy efficiency decreases at higher frequencies. It can be observed that the four-phase clock generators' energy consumption increases more than the two-phase clock generators. This can be attributed to the four-phase clock generator circuit consuming more energy as frequency increases. If we examine the two and four-phase clock generators which are shown in Figure 2.3 and 2.5 we can see that the four-phase clock generator has 4 pairs of PMOS and NMOS to amplify the clock signal while the two-phase clock only has 2. We can model the power consumption of the clock generator circuit using the equation for dynamic power, P = $CV_{dd}^2$f. Thus, we expect the clock generator circuitry of the four-phase clock generator to consume more power as frequency increases.

Temperature variation is an essential component to measure as the operating conditions of integrated circuits can drastically change based on the environment. In this study, we vary the temperature between -20C and 100C and observe its effect on energy consumption. Again, the PRESENT S-Box is used as a base case to help us determine how the changes affect the adiabatic clock generators. The energy results can be seen in Figure 6.2. We can see that energy consumption rises as the temperature rises. This can be attributed to the increase in leakage power of FET-based devices which is a function of temperature. The four-phase clock generator is

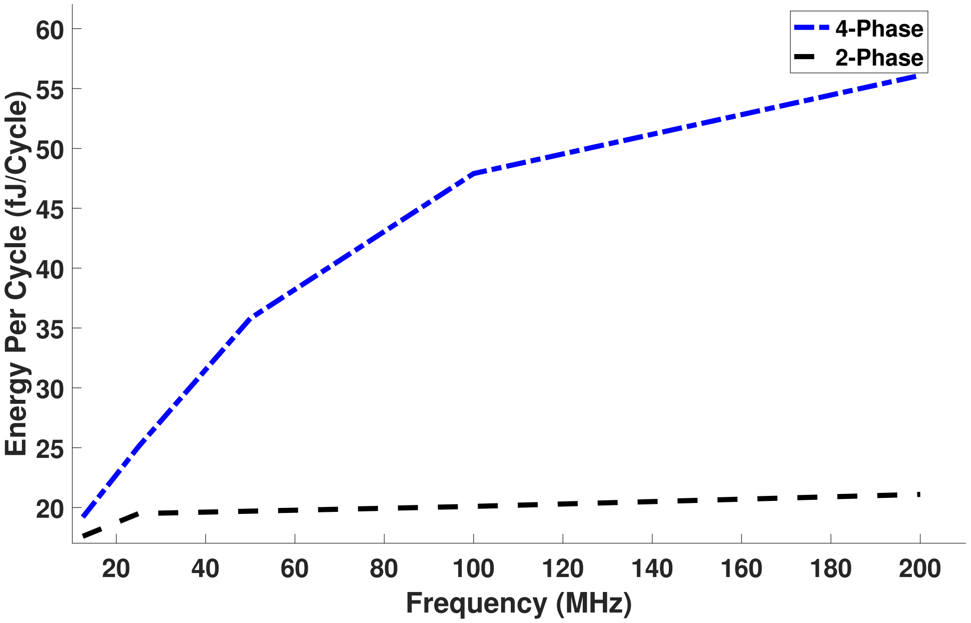


Figure 6.1: Frequency effects on energy per cycle of two and four-phase clock generator.

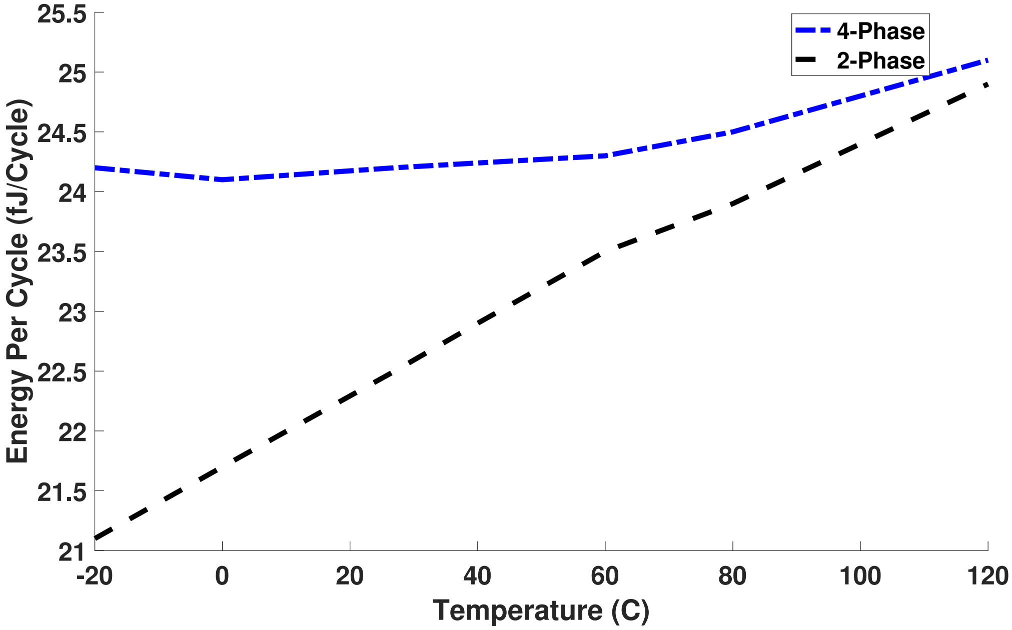


Figure 6.2: Temperature effects on energy per cycle of two and four-phase clock generator.

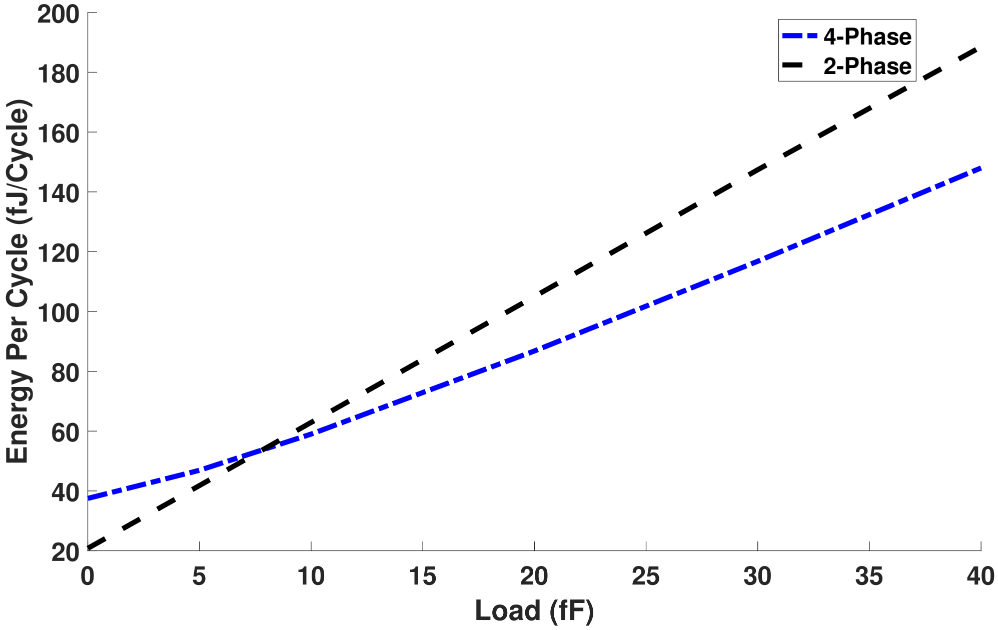


Figure 6.3: Load effects on energy per cycle of two and four-phase clock generator.

more resilient to temperature effects on energy consumption. The reason for this is that the inductance value of the four-phase clock is much lower than the inductance value of the two-phase clock as a result of how resonant frequency is determined. Inductors with lower inductance tend to not be affected by temperature more than those with higher inductance values. The two-phase inductance is much higher and thus varies substantially with temperature. This can lead to degrading Q-factors of the inductor and thus reduced energy efficiency.

A load of an adiabatic circuit can vary substantially across an integrated circuit thus it is important to observe this effect on energy consumption. We vary the load capacitance of the circuit between 0 and 40fF and assume that each output has equal load capacitance. The energy consumption of both two and four-phase adiabatic clock generators is shown in Figure 6.3. We can see that at low capacitive loads, the two-phase adiabatic circuit consumes less energy. However, at higher loads, the four-phase adiabatic circuit consumes less energy. We theorize this is the case because higher capacitance on the loads means more energy can be recovered. The recover and wait phase of the four-phase clock generator is more defined than the recover phase of the two-phase adiabatic clock generator which allows for more recovery of the load charge.

### 6.1.2 Effect of Clock Generator on Power Analysis Attack Resistant Adiabatic Circuits

Adiabatic circuits can be designed in such a way that they are resistant to power analysis attacks. Generally, they are designed to hide variation in power consumption, and thus the ideal power consumption is uniform no matter the data. The adiabatic

Table 6.2: Normalized Energy Deviation and Normalized Standard Deviation values 2 and 4-phase EE-SPFAL AND/NAND

| **Parameter** | **2-Phase** | **4-Phase** |
|---|---|---|
| $E_{min}(fJ)$ | 4.87 | 21.4 |
| $E_{max}(fJ)$ | 5.07 | 21.6 |
| $E_{avg}(fJ)$ | 4.96 | 21.5 |
| $NED(\%)$ | 4.15 | 1.20 |
| $NSD(\%)$ | 1.20 | 0.34 |

clock generators can affect the power consumption and thus can affect variations in power with respect to data. Thus, in this section, we look to compare the 2 and 4-phase adiabatic clock generators with respect to their effect on power analysis attacks.

Basic logic gates such as the XOR and NAND, are the basic building blocks for any circuit. Thus, we first look at these logic gates as a case study to determine how the clock generator affects how resistant a circuit is to power analysis attacks. As discussed in chapter 2, we utilize Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) to quantify how resilient a circuit is to power analysis attacks. The lower NED and NSD the less variation in power a circuit has.

Table 6.2 reports the NED and NSD values of an EE-SPFAL NAND gate implemented with both 2 and 4-phase adiabatic clock generators. The 2-Phase implementation of EE-SPFAL has a NED and NSD of 4.15 and 1.20, respectively. The 4-Phase implementation has a NED and NSD of 1.20 and 0.34, respectively. Table 6.3 reports the NED and NSD values of an EE-SPFAL XOR gate. We can see from Table 6.3 that the 2-Phase XOR has NED and NSD values of 0.119 and 0.060. The 4-Phase implementation has NED and NSD values of 0.014 and 0.007, respectively. Regardless of the circuit, it can be seen that the 4-Phase clock generator results in lower NED and NSD values. This can be attributed to the type of clock and discharge waveform used. The 4-Phase clock generator has the benefit of having the wait phase which means the clock is at GND. This means that the discharge signal can be activated without suffering from non-adiabatic loss. The same cannot be said about the 2-Phase clock generator. There is no defined wait-phase and thus the clock is not at GND when discharge is activated. This results in non-adiabatic loss and thus more variation in power consumption. It should be noted that even with the non-adiabatic loss occurring, the NED and NSD values are still substantially lower than the CMOS NED and NSD values [7].

While evaluating the NED and NSD of logic gates are important, these are not targets of power analysis attacks. Thus, we also look to evaluate the security metrics of the PRESENT S-Box when implemented using 2 and 4-phase clock generators. The S-Box is a typical target for power analysis attacks no matter the encryption algorithm used. Thus, it is important to ensure the power variation is as small as possible for each input. Table 6.4 reports the NED and NSD results for the 2 and 4-phase implementation of the PRESENT S-Box. The 2-Phase implementation of EE-SPFAL resulted in NED and NSD values of 6.83 and 1.23, respectively. The 4-

Table 6.3: Normalized Energy Deviation and Normalized Standard Deviation values 2 and 4-phase EE-SPFAL XOR/XNOR.

| **Parameter** | **2-Phase** | **4-Phase** |
|---|---|---|
| $E_{min}(fJ)$ | 4.80 | 21.35 |
| $E_{max}(fJ)$ | 4.81 | 21.35 |
| $E_{avg}(fJ)$ | 4.81 | 21.35 |
| $NED(\%)$ | 0.119 | 0.014 |
| $NSD(\%)$ | 0.060 | 0.007 |

Table 6.4: Normalized Energy Deviation and Normalized Standard Deviation values 2 and 4-phase EE-SPFAL PRESENT S-Box.

| **Parameter** | **2-Phase** | **4-Phase** |
|---|---|---|
| $E_{min}(fJ)$ | 32.0 | 49.8 |
| $E_{max}(fJ)$ | 34.2 | 51.5 |
| $E_{avg}(fJ)$ | 33.0 | 50.5 |
| $NED(\%)$ | 6.83 | 3.38 |
| $NSD(\%)$ | 1.23 | 0.58 |

Phase implementation resulted in NED and NSD values of 3.38 and 0.58, respectively. Similar to the XOR/XNOR and AND/NAND NED and NSD results, the 4-Phase implementation has lower NED and NSD values. Again, this can be attributed to the 4-Phase clock signals having a defined phase in which the clock is at GND and thus there is reduced non-adiabatic loss.

### Correlation Power Analysis Attack on Adiabatic Circuits Using 2 and 4-Phase Adiabatic Clock Generators

While it is important to quantify how secure a countermeasure is against power analysis attacks, it is also important to perform an attack on the countermeasures. There have been numerous proposed power analysis attack-resistant adiabatic circuits in the literature that utilize 2 and 4-Phase adiabatic clock generators. 2-EE-SPFAL which is presented in Chapter 3 has had a Correlation Power Analysis (CPA) attack performed and successfully prevented the key from being stolen [7]. Degada and Thapliyal have shown that their 2-Phase implementation of SPGAL was also secure against a CPA attack with the clock generator implemented [97]. Degada and Thapliyal have also shown that single-rail adiabatic logic using 2-Phase clock generators also prevents the key from being stolen in a CPA attack [98, 99]. Further, we have also shown that 2-Phase adiabatic clock generators can remain CPA resistant when combined with MTJs by again performing a CPA attack in Chapter 4 [52]. 4-Phase adiabatic clock generators have also been subjects of power analysis attacks and have also been shown to be resistant. Kumar and Thapliyal have developed and performed a Differential Power Analysis (DPA) attack on the 4-Phase implementation of EE-

SPFAL [64]. Kumar and Thapliyal have shown that the key could not be recovered when using their proposed design. Regardless of clock design, it has been shown that performing a power analysis attack is difficult and that adiabatic circuits with their respective clock generators are suitable countermeasures against power analysis attacks.

## 6.2 Conclusion

This chapter has presented a comparison of 2 and 4-Phase adiabatic clock generators in terms of energy efficiency and security against power analysis attacks. The adiabatic clock generator is an important portion of the adiabatic circuit thus it is important to validate these metrics. We have chosen the 2 and 4-Phase clock generators because they are two of the commonly used clocks in adiabatic circuits. Our results show that the 2-Phase adiabatic clock generator has reduced energy consumption when compared with the 4-Phase adiabatic clock generator. In terms of security, we have shown that the 4-Phase adiabatic clock generator has better NED and NSD values than the 2-Phase clock generator. This presents an engineering trade-off between the two clock generators. If energy is the major constraint then the 2-Phase clock generator is preferred while if security is the major constraint, then the 4-Phase clock generator is preferred. Nonetheless, either clock generator results in lower energy consumption than the standard CMOS-based circuits and provides better security against power analysis attacks.

# Chapter 7

# Conclusion and Future Directions

## 7.1 Conclusion

The Internet of Things (IoT) is a collection of devices that share data to perform complex applications. IoT devices improve the ease of life of its users. There are many applications of IoT devices such as within the healthcare field, consumer electronics, industrial manufacturing, etc. While IoT devices have numerous benefits such as increased efficiency of the user, they do have issues that need to be solved. IoT devices are typical targets for both software and hardware-based attacks and thus security is a key issue. Hardware-based attacks such as the Correlation Power Analysis (CPA) attack have been shown to be a dangerous threat to IoT devices. Additional secure hardware is difficult to implement in many IoT devices because they are typically battery operated and thus have a limited energy budget. Therefore, in this dissertation, we have explored the use of low-energy design techniques and emerging memory technologies to design low-energy and secure IoT devices.

Our first contribution was the development of 2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL). EE-SPFAL is an existing CPA-resistant adiabatic logic circuit based on a 4-phase clocking scheme. 4-phase clocking schemes can introduce complex routing and clock designs. Thus, we proposed a 2-phase implementation of EE-SPFAL to reduce said complexity. Further, we have introduced a 2-phase clocking scheme that utilizes the discharge signals of the adiabatic circuit to also act as control signals for the clock generator to further reduce complexity. We have demonstrated that 2-EE-SPFAL has lower energy compared with CMOS equivalent circuits. Further, we have demonstrated that our proposed design is resistant to CPA attacks.

Our second contribution was the development of Energy-Efficient Adiabatic CMOS/MTJ Logic (EE-ACML). Typical bulk-MOSFET and capacitance-storage elements consume high leakage power. Thus, we look to use Magnetic Tunnel Junctions (MTJ) to replace the standard memory elements. MTJs have many benefits such as near-zero leakage power, compatibility with CMOS, high endurance, and low read/write latency. The aforementioned benefits make MTJs a promising choice to replace the standard memory technologies. To that end, we look to combine the dynamic energy savings of adiabatic logic with the many benefits of MTJs (including reduced leakage power) to design an ultra-low energy, CPA-resistant Logic-in-Memory (LiM) architecture.

Our third contribution was the development of a Physically Unclonable Function (PUF) based on both adiabatic logic and MTJs. Again, we look to utilize the dynamic energy-saving properties of adiabatic logic with the leakage energy savings of MTJs to design a low-energy PUF. The proposed PUF utilizes process variation of the MTJs to produce random responses. The proposed PUF was also implemented as a key generator for the lightweight encryption cipher PRESENT.

The final contribution of this dissertation was a comparative study between two and four-phase adiabatic clock generators. The clock generator is an essential component of any adiabatic circuit. Two of the dominating clocking schemes are the two and four-phase clocks. Thus, in this study, we evaluated the clocking schemes to determine which is more applicable to designs in terms of both energy and security. We have determined that the two-phase design has lower energy consumption while the four-phase design has lower Normalized Energy Deviation and Normalized Standard Deviation.

### 7.1.1 Future Work

As more and more complex applications are performed by IoT devices the power requirements are going to increase. This opens up the need for more research developments in low-energy computing. Further, the threat vectors of hardware attacks are going to continue increasing and thus security is an essential component of future IoT device generations. The following items present future work on reducing the energy consumption of IoT devices and improving the security of IoT devices:

1. Adiabatic circuits have been fabricated and verified in laboratory settings for correct functionality and energy efficiency. However, CPA-resistant adiabatic circuits have not been fabricated and tested on their ability to defend against CPA attacks. Thus, this research effort involves fabricating a CPA-resistant adiabatic circuit such as 2-EE-SPFAL and attempting to steal the key through a CPA attack.

   The first problem to solve is how do you fabricate a CPA-resistant adiabatic circuit. An important aspect of CPA-resistant adiabatic circuits is that the evaluation networks are balanced. When the networks are not balanced, data can leak through power consumption. Fabrication of ICs can lead to variation in the transistors and thus information leakage. The questions that need to be solved are how much variation can a CPA-resistant circuit withstand and how can you minimize or hide the variations pre and during fabrication.

2. The second future work is a quantitative analysis of how well a circuit can defend against a power analysis attack. Normalized Energy Deviation and Normalized Standard Deviation are two metrics that allow us to compare different CPA countermeasures. However, these metrics do not tell us how many traces the countermeasure can defend against. For example, in our research studies, we have utilized  12,000 traces in our CPA attack and could not recover the key. However, if we utilize 100,000 traces can we come to the same conclusion? This

research involves determining a method to understand how many traces are necessary to determine if a key can be stolen or if a key can be stolen at all.

3. The third future work involves designing a high-speed, CPA-resistant adiabatic logic circuit. One of the major drawbacks of adiabatic circuits is that they typically operate at lower frequencies. This research work involves designing an adiabatic circuit that works at high frequencies while remaining resistant to CPA attacks.

# Bibliography

[1] Z. Abbas and M. Olivieri, "Impact of technology scaling on leakage power in nano-scale bulk cmos digital standard cells," *Microelectronics Journal*, vol. 45, no. 2, pp. 179–195, 2014.

[2] S. Koley and P. Ghosal, "Addressing hardware security challenges in internet of things: Recent trends and possible solutions," in *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, pp. 517–520, IEEE, 2015.

[3] H. Mahmoodi-Meimand and A. Afzali-Kusha, "Efficient power clock generation for adiabatic logic," in *ISCAS 2001. The 2001 IEEE International Symposium on Circuits and Systems (Cat. No. 01CH37196)*, vol. 4, pp. 642–645, IEEE, 2001.

[4] J. Hu, W. Zhang, X. Ye, and Y. Xia, "Low power adiabatic logic circuits with feedback structure using three-phase power supply," in *Proceedings. 2005 International Conference on Communications, Circuits and Systems, 2005.*, vol. 2, IEEE, 2005.

[5] E. Deng, Y. Zhang, J.-O. Klein, D. Ravelsona, C. Chappert, and W. Zhao, "Low power magnetic full-adder based on spin transfer torque mram," *IEEE Trans. on Magn.*, vol. 49, no. 9, pp. 4982–4987, 2013.

[6] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *Int. workshop on cryptographic hardware and embedded syst.*, pp. 63–80, Springer, 2007.

[7] Z. Kahleifeh and H. Thapliyal, "Adiabatic logic based energy-efficient security for smart consumer electronics," *IEEE Consumer Electronics Magazine*, vol. 11, no. 1, pp. 57–64, 2020.

[8] T. Endoh, H. Koike, S. Ikeda, T. Hanyu, and H. Ohno, "An overview of nonvolatile emerging memories—spintronics for working memories," *IEEE journal on emerging and selected topics in circuits and systems*, vol. 6, no. 2, pp. 109–119, 2016.

[9] S. A. Wolf, J. Lu, M. R. Stan, E. Chen, and D. M. Treger, "The promise of nanomagnetics and spintronics for future logic and universal memory," *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2155–2168, 2010.

[10] B. Tudu and A. Tiwari, “Recent developments in perpendicular magnetic anisotropy thin films for data storage applications,” *Vacuum*, vol. 146, pp. 329–341, 2017.

[11] Y. Wang, H. Cai, L. A. de Barros Naviner, Y. Zhang, X. Zhao, E. Deng, J.-O. Klein, and W. Zhao, “Compact model of dielectric breakdown in spin-transfer torque magnetic tunnel junction,” *IEEE Trans. Electron Devices*, vol. 63, no. 4, pp. 1762–1767, 2016.

[12] Y. Gang, W. Zhao, J.-O. Klein, C. Chappert, and P. Mazoyer, “A high-reliability, low-power magnetic full adder,” *IEEE Trans. Magn.*, vol. 47, no. 11, pp. 4611–4616, 2011.

[13] R. Y. Zhong, X. Xu, E. Klotz, and S. T. Newman, “Intelligent manufacturing in the context of industry 4.0: a review,” *Engineering*, vol. 3, no. 5, pp. 616–630, 2017.

[14] U. Cisco, “Cisco annual internet report (2018–2023) white paper,” *Cisco: San Jose, CA, USA*, 2020.

[15] F. Economics, “The economic impact of iot putting numbers on a revoltuionary technology.”

[16] E. Le Sueur and G. Heiser, “Dynamic voltage and frequency scaling: The laws of diminishing returns,” in *Proceedings of the 2010 international conference on Power aware computing and systems*, pp. 1–8, 2010.

[17] W. C. Athas, L. J. Svensson, J. G. Koller, N. Tzartzanis, and E. Y.-C. Chou, “Low-power digital systems based on adiabatic-switching principles,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 2, no. 4, pp. 398–407, 1994.

[18] H. Mahmoodi-Meimand, A. Afzali-Kusha, and M. Nourani, “Adiabatic carry look-ahead adder with efficient power clock generator,” *IEEE Proc.-Circuits, Devices and Syst.*, vol. 148, no. 5, pp. 229–234, 2001.

[19] S. Yuasa, T. Nagahama, A. Fukushima, Y. Suzuki, and K. Ando, “Giant room-temperature magnetoresistance in single-crystal fe/mgo/fe magnetic tunnel junctions,” *Nature materials*, vol. 3, no. 12, pp. 868–871, 2004.

[20] H.-S. P. Wong, S. Raoux, S. Kim, J. Liang, J. P. Reifenberg, B. Rajendran, M. Asheghi, and K. E. Goodson, “Phase change memory,” *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2201–2227, 2010.

[21] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, “The missing memristor found,” *nature*, vol. 453, no. 7191, pp. 80–83, 2008.

[22] W. Kang, W. Lv, Y. Zhang, and W. Zhao, "Low store power high-speed high-density nonvolatile sram design with spin hall effect-driven magnetic tunnel junctions," *IEEE Trans. Nanotechnol*, vol. 16, no. 1, pp. 148–154, 2016.

[23] W. Kang, Y. Zhang, Z. Wang, J.-O. Klein, C. Chappert, D. Ravelosona, G. Wang, Y. Zhang, and W. Zhao, "Spintronics: Emerging ultra-low-power circuits and systems beyond mos technology," *ACM J. on Emerg. Technol. in Comput. Syst. (JETC)*, vol. 12, no. 2, pp. 1–42, 2015.

[24] A. Hatfield, "Everspin debuts first spin-torque mram for high performance storage systems," *Press relese on webpage of Everspin Technologies, Inc.(www. everspin. com) from 12th*, 2012.

[25] B. Farahani, F. Firouzi, and K. Chakrabarty, "Healthcare iot," in *Intelligent internet of things*, pp. 515–545, Springer, 2020.

[26] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*, pp. 195–212, IEEE, 2017.

[27] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, *et al.*, "Spectre attacks: Exploiting speculative execution," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 1–19, IEEE, 2019.

[28] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, *et al.*, "Meltdown: Reading kernel memory from user space," in *27th USENIX Security Symposium (USENIX Security 18)*, pp. 973–990, 2018.

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

[30] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[31] G. Research, "Iot security primer: Challenges and emerging practices."

[32] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.

[33] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*, pp. 230–234, IEEE, 2014.

[34] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[35] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th international conference for internet technology and secured transactions (IC-ITST)*, pp. 336–341, IEEE, 2015.

[36] A. Shamir and E. Tromer, "Acoustic cryptanalysis," 2004.

[37] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater, and J.-L. Willems, "A practical implementation of the timing attack," in *International Conference on Smart Card Research and Advanced Applications*, pp. 167–182, Springer, 1998.

[38] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *International workshop on cryptographic hardware and embedded systems*, pp. 29–45, Springer, 2002.

[39] S. D. Putra, A. S. Ahmad, S. Sutikno, Y. Kurniawan, and A. D. W. Sumari, "Revealing aes encryption device key on 328p microcontrollers with differential power analysis," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, pp. 5144–5152, 2018.

[40] T. Popp, S. Mangard, and E. Oswald, "Power analysis attacks and countermeasures," *IEEE Design & test of Computers*, vol. 24, no. 6, pp. 535–543, 2007.

[41] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proceedings of the 28th European solid-state circuits conference*, pp. 403–406, IEEE, 2002.

[42] K. Tiri and I. Verbauwhede, "Charge recycling sense amplifier based logic: securing low power security ics against dpa [differential power analysis]," in *Proceedings of the 30th European Solid-State Circuits Conference*, pp. 179–182, IEEE, 2004.

[43] R. S. Pal, S. Sharma, and S. Dasgupta, "Recent trend of finfet devices and its challenges: A review," in *2017 Conference on Emerging Devices and Smart Systems (ICEDSS)*, pp. 150–154, IEEE, 2017.

[44] G. Prenat, K. Jabeur, G. D. Pendina, O. Boulle, and G. Gaudin, "Beyond stt-mram, spin orbit torque ram sot-mram for high speed and high reliability applications," in *Spintronics-based Computing*, pp. 145–157, Springer, 2015.

[45] S. Naik and V. Maral, "Cyber security—iot," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 764–767, IEEE, 2017.

[46] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 148–160, 2002.

[47] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conf.*, pp. 9–14, IEEE, 2007.

[48] Y. Su, J. Holleman, and B. Otis, "A 1.6 pj/bit 96% stable chip-id generating circuit using process variations," in *2007 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*, pp. 406–611, IEEE, 2007.

[49] P. A. Layman, S. Chaudhry, J. G. Norman, and J. R. Thomson, "Electronic fingerprinting of semiconductor integrated circuits," May 18 2004. US Patent 6,738,294.

[50] Z. Kahleifeh and H. Thapliyal, "2-phase energy-efficient secure positive feedback adiabatic logic for cpa-resistant iot devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, pp. 1–5, IEEE, 2020.

[51] Z. Kahleifeh and H. Thapliyal, "Low-energy and cpa-resistant adiabatic cmos/mtj logic for iot devices," in *2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pp. 314–319, IEEE, 2021.

[52] Z. Kahleifeh and H. Thapliyal, "Ee-acml: Energy-efficient adiabatic cmos/mtj logic for cpa-resistant iot devices," *Sensors*, vol. 21, no. 22, p. 7651, 2021.

[53] O. Lo, W. J. Buchanan, and D. Carson, "Power analysis attacks on the aes-128 s-box using differential power analysis (dpa) and correlation power analysis (cpa)," *Journal of Cyber Security Technology*, vol. 1, no. 2, pp. 88–107, 2017.

[54] J.-S. Coron, P. Kocher, and D. Naccache, "Statistics and secret leakage," in *International Conference on Financial Cryptography*, pp. 157–173, Springer, 2000.

[55] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 1, pp. 246–251, IEEE, 2004.

[56] H. Marzouqi, M. Al-Qutayri, and K. Salah, "Review of gate-level differential power analysis and fault analysis countermeasures," *IET Information Security*, vol. 8, no. 1, pp. 51–66, 2013.

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

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

[59] A. Moradi, M. Salmasizadeh, and M. T. M. Shalmani, "Power analysis attacks on mdpl and drsl implementations," in *International Conference on Information Security and Cryptology*, pp. 259–272, Springer, 2007.

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

[61] B.-D. Choi, K. E. Kim, K.-S. Chung, and D. K. Kim, "Symmetric adiabatic logic circuits against differential power analysis," *ETRI journal*, vol. 32, no. 1, pp. 166–168, 2010.

[62] Y. Moon and D.-K. Jeong, "An efficient charge recovery logic circuit," *IEICE transactions on electronics*, vol. 79, no. 7, pp. 925–933, 1996.

[63] C. Monteiro, Y. Takahashi, and T. Sekine, "Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level," *Microelectronics Journal*, vol. 44, no. 6, pp. 496–503, 2013.

[64] S. D. Kumar, H. Thapliyal, and A. 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*, vol. 7, no. 2, pp. 281–293, 2016.

[65] A. Blotti, S. Di Pascoli, and R. Saletti, "Simple model for positive-feedback adiabatic logic power consumption estimation," *Electronics Letters*, vol. 36, no. 2, pp. 116–118, 2000.

[66] J. S. Moodera, L. R. Kinder, T. M. Wong, and R. Meservey, "Large magnetoresistance at room temperature in ferromagnetic thin film tunnel junctions," *Physical Review Lett.*, vol. 74, no. 16, p. 3273, 1995.

[67] R. Zand, A. Roohi, S. Salehi, and R. F. DeMara, "Scalable adaptive spintronic reconfigurable logic using area-matched mtj design," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 63, no. 7, pp. 678–682, 2016.

[68] B. Behin-Aein, J.-P. Wang, and R. Wiesendanger, "Computing with spins and magnets," *MRS Bulletin*, vol. 39, no. 8, pp. 696–702, 2014.

[69] A. D. Kent, "Perpendicular all the way," *Nature materials*, vol. 9, no. 9, pp. 699–700, 2010.

[70] R. W. Dave, G. Steiner, J. Slaughter, J. Sun, B. Craigo, S. Pietambaram, K. Smith, G. Grynkewich, M. DeHerrera, J. Akerman, *et al.*, "Mgo-based tunnel junction material for high-speed toggle magnetic random access memory," *IEEE Trans. Magn.*, vol. 42, no. 8, pp. 1935–1939, 2006.

[71] S. Matsunaga, J. Hayakawa, S. Ikeda, K. Miura, T. Endoh, H. Ohno, and T. Hanyu, "Mtj-based nonvolatile logic-in-memory circuit, future prospects and issues," in *2009 Design, Automation & Test in Europe Conference & Exhibition*, pp. 433–435, IEEE, 2009.

[72] P. Barla, V. K. Joshi, and S. Bhat, "A novel low power and reduced transistor count magnetic arithmetic logic unit using hybrid stt-mtj/cmos circuit," *IEEE Access*, vol. 8, pp. 6876–6889, 2020.

[73] S. D. Kumar, Z. Kahleifeh, and H. Thapliyal, "Novel secure mtj/cmos logic (smcl) for energy-efficient and dpa-resistant design," *SN Computer Science*, vol. 2, no. 2, pp. 1–10, 2021.

[74] C. Labrado, "Energy harvesting and sensor based hardware security primitives for cyber-physical systems," 2021.

[75] A. Degada, "Designing novel hardware security primitives for smart computing devices," 2021.

[76] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symp. on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)*, pp. 176–179, IEEE, 2004.

[77] B. L. P. Gassend, *Physical random functions*. PhD thesis, Massachusetts Institute of Technology, 2003.

[78] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic pufs from flip-flops on reconfigurable devices," in *3rd Benelux workshop on information and system security (WISSec 2008)*, vol. 17, p. 2008, 2008.

[79] W. C. Athas, L. Svensson, and N. Tzartzanis, "A resonant signal driver for two-phase, almost-non-overlapping clocks," in *1996 IEEE International Symposium on Circuits and Systems. Circuits and Systems Connecting the World. ISCAS 96*, vol. 4, pp. 129–132, IEEE, 1996.

[80] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *Int. workshop on cryptographic hardware and embedded systems*, pp. 450–466, Springer, 2007.

[81] J. Wu, Y. Shi, and M. Choi, "Measurement and evaluation of power analysis attacks on asynchronous s-box," *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 10, pp. 2765–2775, 2012.

[82] F. Ren, *Energy-performance characterization of CMOS/magnetic tunnel junction (MTJ) hybrid logic circuits*. PhD thesis, Citeseer, 2010.

[83] T. Ju, Z. Chunlian, *et al.*, "Mlp-based power analysis attacks with two-point joint feature selection," in *2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp. 250–254, IEEE, 2020.

[84] S. Sahay and M. Suri, "Recent trends in hardware security exploiting hybrid cmos-resistive memory circuits," *Semiconductor Science and Technology*, vol. 32, no. 12, p. 123001, 2017.

[85] A. Asenov, S. Kaya, and J. H. Davies, "Intrinsic threshold voltage fluctuations in decanano mosfets due to local oxide thickness variations," *IEEE Trans. Electron Devices*, vol. 49, no. 1, pp. 112–119, 2002.

[86] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable spin-transfer torque magnetic ram-based physical unclonable function with multi-response-bits per cell," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1630–1642, 2015.

[87] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 13, no. 10, pp. 1200–1205, 2005.

[88] S. Stanzione, D. Puntin, and G. Iannaccone, "Cmos silicon physical unclonable functions based on intrinsic process variability," *IEEE J. Solid-State Circuits*, vol. 46, no. 6, pp. 1456–1463, 2011.

[89] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based puf," in *IEEE Int. symp. of circuits and systems (ISCAS)*, pp. 2071–2074, IEEE, 2011.

[90] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid ro puf with improved thermal stability for lightweight applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*, vol. 34, no. 7, pp. 1143–1147, 2015.

[91] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "14.2 a physically unclonable function with ber¡ 10- 8 for robust chip authentication using oscillator collapse in 40nm cmos," in *IEEE Int. Solid-State Circuits Conf. Digest of Technical Papers*, pp. 1–3, IEEE, 2015.

[92] A. Neale and M. Sachdev, "A low energy sram-based physically unclonable function primitive in 28 nm cmos," in *IEEE Custom Integrated Circuits Conf. (CICC)*, pp. 1–4, IEEE, 2015.

[93] S. Tao and E. Dubrova, "Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm cmos," *Electronics Lett.*, vol. 52, no. 10, pp. 805–806, 2016.

[94] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Optimizating emerging nonvolatile memories for dual-mode applications: Data storage and key generator," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*, vol. 34, no. 7, pp. 1176–1187, 2015.

[95] S. D. Kumar and H. Thapliyal, "Design of adiabatic logic-based energy-efficient and reliable puf for iot devices," *ACM J. on Emerging Technologies in Computing Systems (JETC)*, vol. 16, no. 3, pp. 1–18, 2020.

[96] S. B. Dodo, R. Bishnoi, S. M. Nair, and M. B. Tahoori, "A spintronics memory puf for resilience against cloning counterfeit," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 27, no. 11, pp. 2511–2522, 2019.

[97] A. Degada and H. Thapliyal, "2-spgal: 2-phase symmetric pass gate adiabatic logic for energy-efficient secure consumer iot," in *2021 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, IEEE, 2021.

[98] A. Degada and H. Thapliyal, "2-phase adiabatic logic for low-energy and cpa-resistant implantable medical devices," *IEEE Transactions on Consumer Electronics*, 2022.

[99] A. Degada and H. Thapliyal, "Single-rail adiabatic logic for energy-efficient and cpa-resistant cryptographic circuit in low-frequency medical devices," *IEEE Open Journal of Nanotechnology*, vol. 3, pp. 1–14, 2021.

Vita

## Education

University of Kentucky, Lexington, Kentucky, USA
Bachelors of Science, Computer Engineering, December 2018

## Awards

1. Received “Best Paper Presentation Award - Second Place” at IEEE 6th World Forum on Internet of Things, 2020, for our paper titled, “2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic for CPA Resistant IoT Devices”.

2. Received ”Outstanding Student Paper Award” at IEEE 6th World Forum on Internet of Things, 2020, for our paper titled, “2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic for CPA Resistant IoT Devices”.

3. Received ”Engineering Outstanding Master’s Student” from the University of Kentucky College of Engineering.

4. Received ”Outstanding Masters Student Research Award” from the University of Kentucky Department of Electrical and Computer Engineering

5. Received ”Outstanding Undergraduate Research Award” from the University of Kentucky Department of Electrical and Computer Engineering

## Invention Disclosure

1. Novel Design of 2-Phase Secure Adiabatic Circuits for Consumer IoT Devices, H. Thapliyal, Z. Kahleifeh and A. Degada, Invention Disclosure, University of Kentucky, (UK-2572), Feb 2021.

## Publications

1. Kahleifeh, Zachary, and Himanshu Thapliyal. ”EE-ACML: Energy-Efficient Adiabatic CMOS/MTJ Logic for CPA-Resistant IoT Devices.” Sensors 21.22 (2021): 7651.

2. Kahleifeh, Zachary, and Himanshu Thapliyal. ”Low-Energy and CPA-Resistant Adiabatic CMOS/MTJ Logic for IoT Devices.” 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2021.

3. Kumar, S. Dinesh, Zachary Kahleifeh, and Himanshu Thapliyal. ”Novel Secure MTJ/CMOS Logic (SMCL) for Energy-Efficient and DPA-Resistant Design.” SN Computer Science 2.2 (2021): 1-10.

4. Kahleifeh, Zachary, and Himanshu Thapliyal. ”Adiabatic logic based energy-efficient security for smart consumer electronics.” IEEE Consumer Electronics Magazine 11.1 (2020): 57-64.

5. Kahleifeh, Zachary, and Himanshu Thapliyal. ”2-phase energy-efficient secure positive feedback adiabatic logic for cpa-resistant iot devices.” 2020 IEEE 6th World Forum on Internet of Things (WF-IoT). IEEE, 2020.

6. Thapliyal, Himanshu, and Zachary Kahleifeh. ”Approximate energy recovery 4-2 compressor for low-power sub-GHz IoT applications.” 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2019.

7. Thapliyal, Himanshu, and Zachary Kahleifeh. ”Solving energy and cybersecurity constraints in IoT devices using energy recovery computing.” Proceedings of the 2019 on Great Lakes symposium on VLSI. 2019.

8. Kahleifeh, Zach, S. Dinesh Kumar, and Himanshu Thapliyal. ”Hardware Trojan detection in implantable medical devices using adiabatic computing.” 2018 IEEE International Conference on Rebooting Computing (ICRC). IEEE, 2018.

Zachary Kahleifeh