2021

Designing Novel Hardware Security Primitives for Smart Computing Devices

Amitkumar Degada
University of Kentucky, amitdegada@gmail.com
Author ORCID Identifier:
https://orcid.org/0000-0002-6335-694X
Digital Object Identifier: https://doi.org/10.13023/etd.2021.441

STUDENT AGREEMENT:

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

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

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

REVIEW, APPROVAL AND ACCEPTANCE

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

Amitkumar Degada, Student

Dr. Himanshu Thapliyal, Major Professor

Dr. Daniel Lau, Director of Graduate Studies

DESIGNING NOVEL HARDWARE SECURITY PRIMITIVES FOR SMART COMPUTING 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
Amitkumar Dalpatray Degada
Lexington, Kentucky
Director: Dr. Himanshu Thapliyal, Associate Professor of
Electrical and Computer Engineering
Lexington, Kentucky
2021

ORCID: 0000-0002-6335-694X

ABSTRACT OF DISSERTATION

DESIGNING NOVEL HARDWARE SECURITY PRIMITIVES
FOR SMART COMPUTING DEVICES

Smart computing devices are miniaturized electronics devices that can sense their surroundings, communicate, and share information autonomously with other devices to work cohesively. Smart devices have played a major role in improving quality of the life and boosting the global economy. They are ubiquitously present, smart home, smart city, smart girds, industry, healthcare, controlling the hazardous environment, and military, etc. However, we have witnessed an exponential rise in potential threat vectors and physical attacks in recent years. The conventional software-based security approaches are not suitable in the smart computing device, therefore, hardware-enabled security solutions have emerged as an attractive choice. Developing hardware security primitives, such as True Random Number Generator (TRNG) and Physically Unclonable Function (PUF) from electrical properties of the sensor could be a novel research direction. Secondly, the Lightweight Cryptographic (LWC) ciphers used in smart computing devices are found vulnerable against Correlation Power Analysis (CPA) attack. The CPA performs statistical analysis of the power consumption of the cryptographic core and reveals the encryption key. The countermeasure against CPA results in an increase in energy consumption, therefore, they are not suitable for battery operated smart computing devices.

The primary goal of this dissertation is to develop novel hardware security primitives from existing sensors and energy-efficient LWC circuit implementation with CPA resilience. To achieve these. we focus on developing TRNG and PUF from existing photoresistor and photovoltaic solar cell sensors in smart devices Further, we explored energy recovery computing (also known as adiabatic computing) circuit design technique that reduces the energy consumption compared to baseline CMOS logic design and same time increasing CPA resilience in low-frequency applications, e.g. wearable fitness gadgets, hearing aid and biomedical instruments.

The first contribution of this dissertation is to develop a TRNG prototype from the uncertainty present in photoresistor sensors. The existing sensor-based TRNGs suffer a low random bit generation rate, therefore, are not

suitable in real-time applications. The proposed prototype has an average random bit generation rate of 8 kbps, 32 times higher than the existing sensor-based TRNG. The proposed lightweight scrambling method results in random bit entropy close to ideal value 1. The proposed TRNG prototype passes all 15 statistical tests of the National Institute of Standards and Technology (NIST) Statistical Test Suite with quality performance.

The second contribution of this dissertation is to develop an integrated TRNG-PUF designed using photovoltaic solar cell sensors. The TRNG and PUF are mutually independent in the way they are designed, therefore, integrating them as one architecture can be beneficial in resource-constrained computing devices. We propose a novel histogram-based technique to segregate photovoltaic solar cell sensor response suitable for TRNG and PUF respectively. The proposed prototype archives approximately 34% improvement in TRNG output. The proposed prototype achieves an average of 92.13% reliability and 50.91% uniformity performance in PUF response. The proposed sensor-based hardware security primitives do not require additional interfacing hardware. Therefore, they can be ported as a software update on existing photoresistor and photovoltaic sensor-based devices. Furthermore, the sensor-based design approach can identify physically tempered and faulty sensor nodes during authentication as their response bit differs.

The third contribution is towards the development of a novel 2-phase sinusoidal clocking implementation, 2-SPGAL for existing Symmetric Pass Gate Adiabatic Logic (SPGAL). The proposed 2-SPGAL logic-based LWC cipher PRESENT shows an average of 49.34% energy saving compared to baseline CMOS logic implementation. Furthermore, the 2-SPGAL prototype has an average of 22.76% better energy saving compared to 2-EE-SPFAL (2-phase Energy-Efficient-Secure Positive Feedback Adiabatic Logic). The proposed 2-SPGAL was tested for energy-efficiency performance for the frequency range of 50 kHz to 250 kHz, used in healthcare gadgets and biomedical instruments. The proposed 2-SPGAL based design saves 16.78% transistor count compared to 2-EE-SPFAL counterpart.

The final contribution is to explore Clocked CMOS Adiabatic Logic (CCAL) to design a cryptographic circuit. Previously proposed 2-SPGAL and 2-EE-SPFAL uses two complementary pairs of the transistor evaluation network, thus resulting in a higher transistor count compared to the CMOS counterpart. The CCAL structure is very similar to CMOS and unlike 2-SPGAL and 2-EE-SPFAL, it does not require discharge circuitry to improve security performance. The case-study implementation LWC cipher PRESENT

S-Box using CCAL results into 45.74% and 34.88% transistor count saving compared to 2-EE-SPFAL and 2-SPGAL counterpart. Furthermore, the case-study implementation using CCAL shows more than 95% energy saving compared to CMOS logic at frequency range 50 kHz to 125 kHz, and approximately 60% energy saving at frequency 250 kHz. The case study also shows 32.67% and 11.21% more energy saving compared to 2-EE-SPFAL and 2-SPGAL respectively at frequency 250 kHz. We also show that 200 fF of tank capacitor in the clock generator circuit results in optimum energy and security performance in CCAL.

KEYWORDS: Hardware Security Primitives, True-Random Number Generator, Physically Unclonable Functions, Adiabatic Logic, Cryptography, Medical Devices, Side-Channel Attack, Correlation Power Analysis Attack.

Amitkumar Dalpatray Degada

December 10, 2021

DESIGNING NOVEL HARDWARE SECURITY PRIMITIVES
FOR SMART COMPUTING DEVICES

By

Amitkumar Dalpatray Degada

Dr. Himanshu Thapliyal

(Director of Dissertation)

Dr. Daniel Lau

(Director of Graduate Studies)

December 10, 2021

(Date)

Dedicated to my Teachers

Thanks for leading me from the darkness of ignorance
to the quest for the immortality of knowledge.

ACKNOWLEDGEMENTS

Once Einstein said that It is the supreme art of the teacher to awaken joy in creative expression and knowledge. I sincerely express my deepest gratitude to my advisor Dr. Himanshu Thapliyal. My research journey would not have been possible without constant encouragement, guidance, and assistance from Dr. Thapliyal. I also thank my committee members, Dr. Hank Dietz, Dr. D. Manivannan, and Dr. Bruce Walcott for their insightful suggestions to improve my research. I am deeply grateful to Dr. Dietz for his unwavering support and discussions on computer architecture, which have a deep impact on shaping my thoughts.

I would like to extend my sincere thanks to Dr. Vijay Singh for giving me access to the solar cell research lab for experimental work. My journey at VEDANT's (VLSI Emerging Design And Nano Things Security) lab would not be smooth interactive, and evolving without the support of my colleagues. I heartily thank Zachary Kahleifeh for helping to learn tools, discussions, and feedback. I also thank my lab mate Rajdeep Kumar Nath, Edgard Munoz-Coreas, Carson Labrado, and Wu Yang for their inputs, help, and support.

No words are enough to express the unconditional love of the parents.I am forever thankful to my father for nurturing patience, leadership quality, and being the example of performing one's duties without any expectations. I also thank my mother for her love and prayers. I also express my profound gratitude to my Grandparents, family members, and well-wishers for their unceasing support and encouragement.

I take this opportunity to thank my sister Donata. Before starting the Ph.D., situations and surroundings asked me to quit my dream. My sister instilled the faith back in me and this dissertation would not be possible without her unconditional love and encouragement. I thank my brother, Akshay for his unparalleled support and for smoothly taking over my social responsibilities. I also thank my friends, Praneeth, Jujube, and Sairam for creating many laughter moments and memorable cooking sessions.

Lastly, I thank my Mahadev, I bow down to you. I feel that I am nothing, it is just his blessing that makes things work. I am also deeply grateful to all the yogis, and spiritual masters who came across my path of life. I thank them for answering my questions to know the purpose of life, realizing me to see the beauty in everything, and steering me to be in union with divine energy. This has a deep impact on the success of this dissertation.

This work was supported by National Science Foundation grant 1738662
and National Science Foundation career award No. 1845448.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In recent years, we have seen the proliferation of handheld portable smart electronic devices. They have contributed significantly to improving our quality of the life and our life has become inseparable from such "smart" devices. The smart devices find applications in smart healthcare, smart home, manufacturing, power generation, military, and controlling hazardous environment [12] [13]. The growth in the semiconductor industry, machine learning, algorithms, and networking is driving them to widen the spectrum of applications. It is expected by the year 2025, there will be a total of 45.9 billion smart devices [14], [15], [16]. In other words, there will be on average at least 6 to 7 devices per person. Further, it is expected that the above figure will certainly be higher in coming years in the US and many European Nations.

Smart devices are often compact, have limited computational power, smaller memory, and finite energy budget (i.e. battery operated). Therefore, they are also referred to as resource-constrained devices. Further, they are deployed at the very last end in the user domain. The broad definition of such smart devices includes Internet-of-Things (IoT), wireless sensor nodes, RFID tags, personal healthcare devices, smart biomedical instruments, and Cyber-Physical Systems (CPS). Such devices often include sensors to collect information, communicate with each other to work cohesively and execute functions with minimal human interaction.

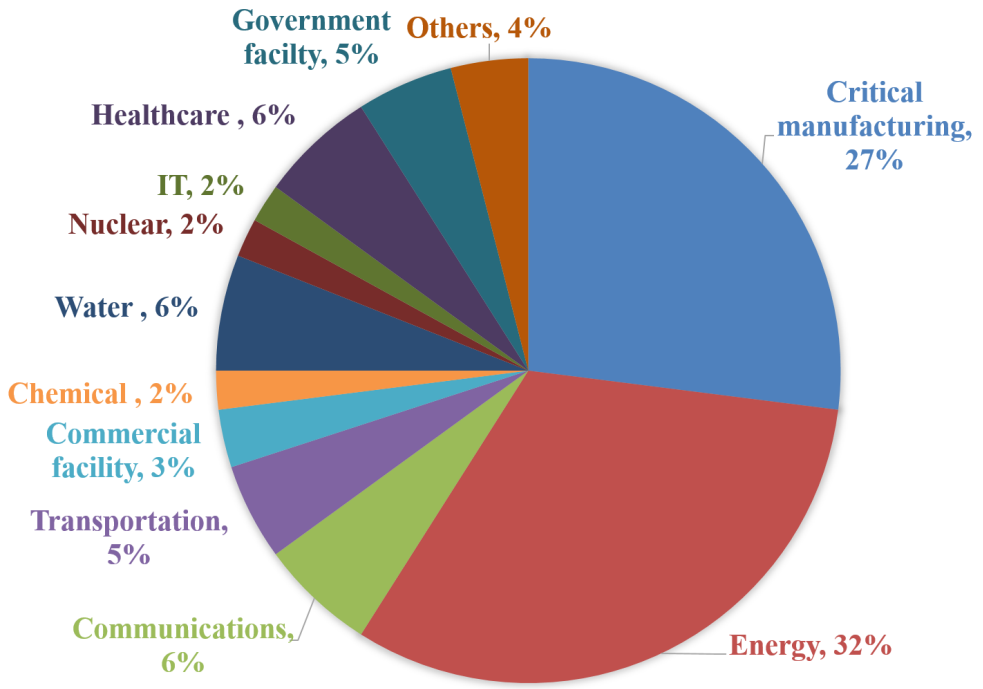

Figure 1.1: Percentage of cyber-attacks responded by ICS-CERT [1].

The cyber-security experts have always raised the alarm on exploitation of unsecured smart device connected to Internet [17] [18] [19] [20]. The data shown in Figure 1.1 is based on a report [1] published by Industrial Control System (ICS) Cyber Emergency Response Team (CERT). According to a recent report published by Nokia, IoT devices are responsible for 32.72% of total cyber attacks in the year 2020 compare to 16.17% in 2019 [21]. The attacks on financial sectors result in monetary loss, similarly, attacks on manufacturing could be hampered, and attacks on transportation may affect timely delivery. However, the attacks on healthcare devices could threaten the life of the patient. In recent COVID-19 pandemic has seen 600% increment in phishing in March 2020 and attempts have been made to disrupt the health-care infrastructure [22]. As the shift to work-from-home began then the number of attacks on IoT devices incremented up to 46% first six months and more than half (55.74%) of IoT networks experienced port-scan attack [23]. Kevin Ashton, who coined the word Internet-of-Things first time in 2009 [24], would not have imagined that the glimpse of such a rise of security concern in a decade.

1.1 Motivation

The application of the smart devices has shown unquestionable potential to transform human well-being. However, they are not perfectly flawless. There exist many surveys in research literature which have reported various security attacks possible on smart devices, e.g. IoT, CPS and biomedical devices [18] [19] [25] [26][27] [28] [29] [30] [31] [32] [33]. The above work in literature points out that the constrained computational power, limited memory size, relying on battery, lower costs and wide deployment at the user end has given exponential rise in cyberattacks on smart devices.

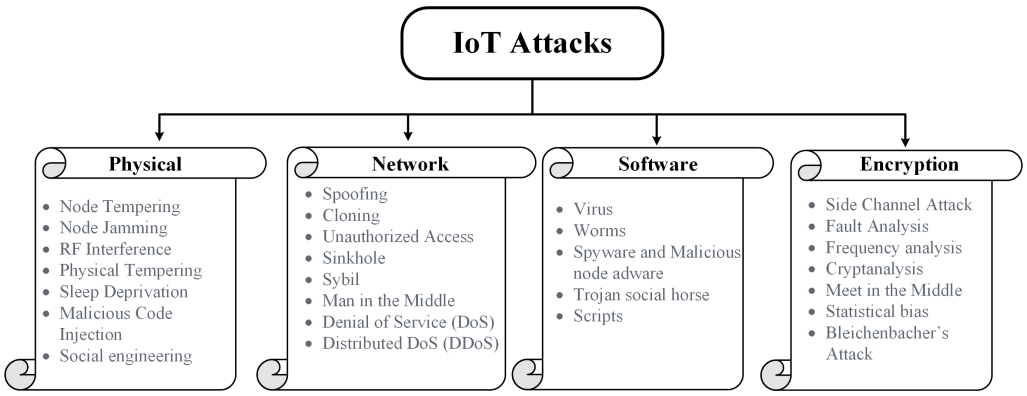

Figure 1.2: Classifications of the IoT attacks [2].

It is reported in [34] that 98% of IoT data is unencrypted. It has been shown that it is very easy for an attacker to bypass the front defense line via a phishing attack and get access to unencrypted user information and exploit it later (Figure 1.2). Many incidents have been reported showing the breach of security in IoT devices. The "Jeep Hack" demonstrated by Dr. Miller and Chris Valasek is one of the most widely discussed and popular examples. They demonstrated the vulnerabilities in sensor communication over CAN bus and infotainment system allow to take remote control of the vehicle [35]. This resulted in the recall of 1.4 million vehicles. The researcher in [36] has shown that a correlation power analysis attack (discussed in more detail in Section 2.6) can be used to identify the encryption key in the smart lamp. Later, a compromised IoT node can infect the other nodes in the network, and chain reaction enables the attacker to create a massive DDoS (Distributed Denial Service Attack). Similarly, the usage of correlation power analysis

to identify the key in the South Korean public transit system. Later, it was used to mutually authenticate the transit card and recharge the balance without any payment. The above incidents imply that a careless security implementation can have dire effects on the future success of IoT devices.

Cyber-Physical Systems (CPS) are a full-fledged network of smart devices often employed to take input from the physical world and control the surrounding environment. Research and statistics estimated by Gartner Inc state that by the year 2023, the financial impacts of the Cyber-Physical attacks are likely to reach more than 50 billion US dollars [37]. Further, their close operation to control the physical environment can result in human fatalities. The insurance, compensation given for loss of life, fines by regulatory bodies, and litigation fees, if included, then the above figure would certainly be higher. It is not only financial losses, the loss of human lives can eclipse brand reputation and permanent loss of trust among customers. The Cybersecurity and Infrastructure Security Agency (CISA) under the US Department of Homeland Security, publish alerts and advisory on several cyber-physical attacks from time to time [38]. The above list cyberattacks on critical infrastructure, e.g. Electric grid, municipal transportation agencies, HVAC systems, water, and oil distribution systems, and nuclear plants.

The Healthcare sector has an inherent weakness in security infrastructure deployment. Alone in the US, over 110 million patients and 81% of healthcare organizations reported the compromise of their data in 2016 [39]. The healthcare sector is always an always hot favorite target for two primary reasons. First, it is a heterogeneous system having reliance on third-party biomedical instruments, communication and networking infrastructure, and HVAC, etc. Second, the hacked data is valuable and reach. The medical records of the patient not only contain healthcare reports and credit card information, rather, multiple and permanent identifiers that cannot be reset. Many of the biomedical instrumentation are designed using older technology and can become an entry point to the healthcare infrastructure. Therefore, there is a need to secure biomedical devices used in the diagnostic process, e.g. Magnetic Particle Imaging, Electrical Impedance Myography, Electrical Impedance Tomography, bioelectrical impedance meter, etc.

Further, the advancement in semiconductor technology and algorithms development (e.g. Machine Learning, Deep-Learning) have empowered the inclusion of implantable medical devices, hearing aid, and fitness tracker devices. The above devices are battery operated and their lie span is limited. Further, their limited computing power and connectivity to the communi-

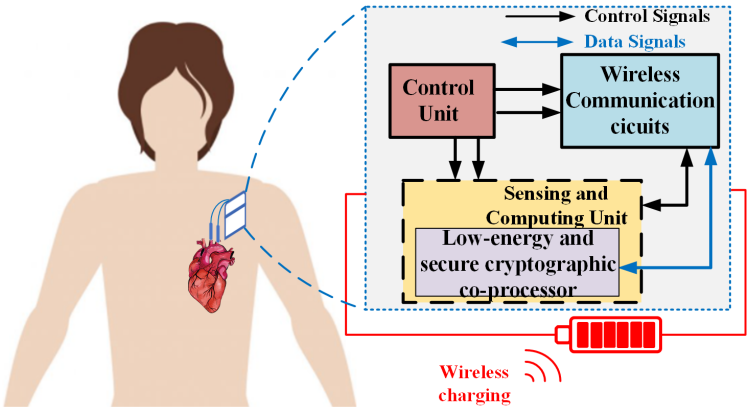

Figure 1.3: Modern implantable medical devices requires low-energy consumption and secure cryptographic circuits.

cation network makes them easy target (Figure 1.3). In research literature, it has been already shown that compromised node can perform unauthorized command execution, data transmission [40], deplete the battery [41] and generating electrical shocks [42] [43]. The compromised security not only results in data and identity being stolen, however, but it could also be life-threatening in some cases. The proposed solution to combat the above security challenges comes at the cost of increased power consumption. Therefore, the security solutions proposed for battery-operated healthcare devices should be energy-efficient.

To summarize, smart devices are going to be more and more widespread as we move towards the future of smart cities, smart agriculture, smart traffic management, autonomous vehicles, telemedicine, and smart biological devices. Smart systems, e.g. IoT, CPS, and connected biomedical devices have an almost identical infrastructure setup that includes one or more sensors, a computing unit, communication, and networking infrastructure, and an actuator to control the output. The attack surface on such devices is going more and more and a new paradigm shift should be incorporated. In recent years, researchers have remolded their focus to include hardware-enabled solutions. The primary focus of this dissertation report is to develop security solutions at the hardware level to strengthen the security infrastructure in resource-constrained devices.

1.2 Hardware Enabled Solution in Smart Computing Security framework

Smart devices require the sound implementation of the cryptographic framework to ensure the level of trust in confidentiality, integrity, and availability. The security threats in resource-constrained devices can not only be looked at in conventional software approaches. The limitation of the resource-constrained devices and increased challenges due to growing attack vectors have inspired researchers to design hardware-enabled solutions. The cryptographic operations performed in smart devices can be grouped under a cryptographic coprocessor (Figure 1.4). The cryptographic coprocessor is responsible for secure key generation, safely protecting the keys, managing the keys, performing cryptographic operations, e.g. encryption, decryption, hashing, and digital signature.

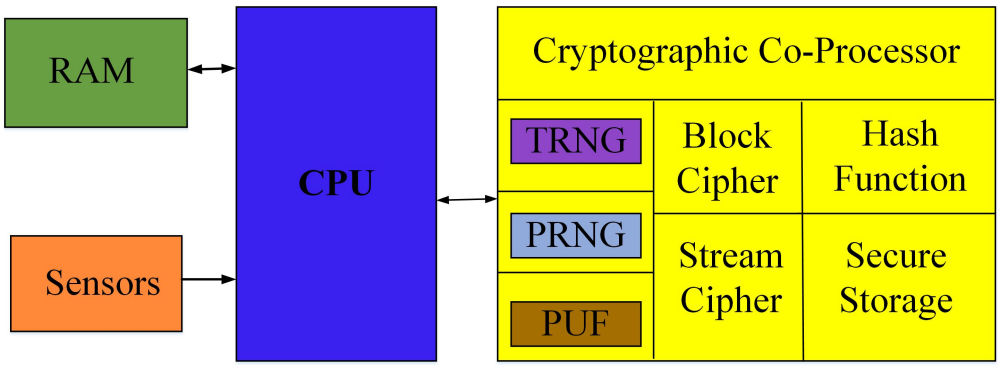

Figure 1.4: Hardware security primitives in security framework of smart computing devices .

The hardware security primitives are the components that operate at the root level (i.e. hardware) in the security infrastructure pyramid and have a dedicated role. True Random Number Generator (TRNG), Physically Unclonable Function (PUF), block cipher, and stream ciphers are examples of cyber security primitives. The hardware security primitives, such as TRNG and PUF come as a plug-and-play module. In the existing literature, many stand-alone TRNG and PUF design based have been proposed [44] [45] [46] [47]. Adopting such dedicated solutions in resource-constrained devices is not suitable.

The smart devices used in IoT, biomedical applications, and CPS have some common features. They often include one or more sensors, a computing unit, communication infrastructure, and an actuator. In this research, we proposed a novel way to design hardware security primitives using the electrical response of the sensor and its interfacing to the computing unit. The proposed solutions in this report are suitable for resource-constrained devices and do not require additional interfacing hardware from sensors and computing units. The above approach results in space-saving and direct porting of proposed hardware security primitives in existing sensor-based smart computing devices.

Designing the hardware security primitives can prevent tempering and malicious replacement of the sensor. The proposed TRNG and PUF modules in the report use the electrical response of the sensor as an entropy source. It is important to note that if an attacker compromise sensor tempered physically or replaced by a malicious one, then it will not result in the same response producing different output. The above feature enables the identification of faulty or compromised nodes easily during the authentication process.

To present the importance of sensor-based TRNG and PUF, let's look at some information in the IoT domain. Figure 1.6 illustrates information compiled from data published in white paper [34] by Palo Alto Networks. It is very surprising to see that camera only constitutes 5% of IoT devices, however, they are responsible for 33% of total reported security vulnerabilities. further, the consumer electronics and energy devices contribute 7% and 6% of total vulnerabilities reported. In summary, 46% of IoT security vulnerabilities comes from camera, consumer electronics, and energy devices.

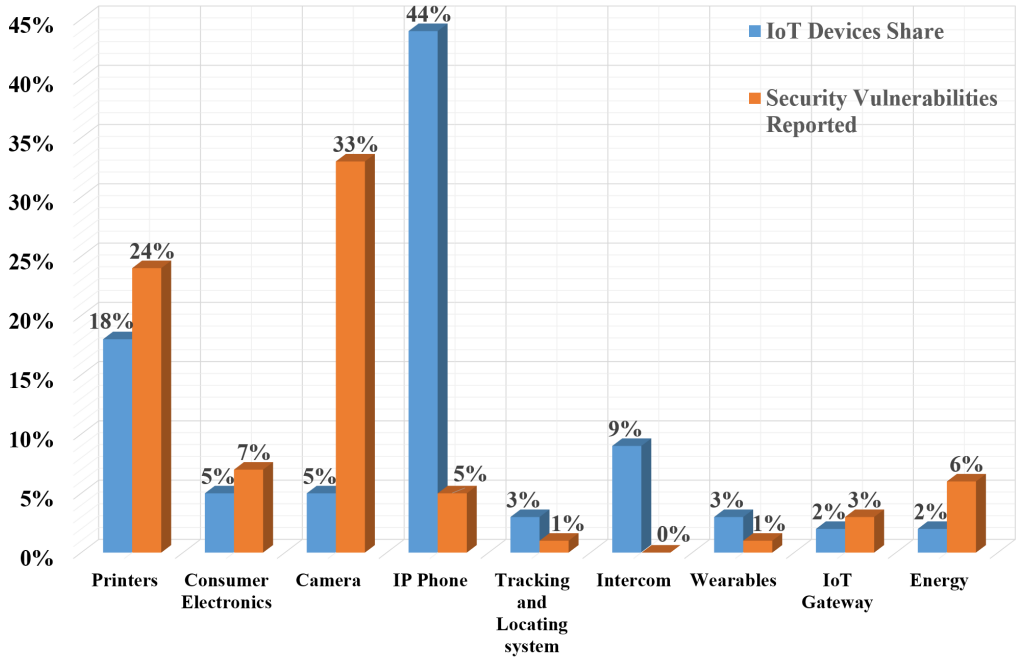

Figure 1.5: IoT Device share and reported security vulnerabilities.

The photoresistor sensor exhibits a change in electrical resistance according to ambient light conditions. It is widely used to activate lights in smart homes, smart street lighting, phototaxic navigation in robotic tadpoles, intelligent brightness and contrast control in smart televisions, calculating shutter speed in smart cameras, infrared astronomy, infrared spectroscopy, and optical coding. On the other hand, The PV solar cell sensor is the most preferred mechanism of energy harvesting for mobile IoT devices [48]. Designing TRNG and PUF using photoresistors and photovoltaic solar cell sensors can be beneficial in many smart devices. Therefore, In this research, we explored a novel approach to design TRNG and PUF by exploring the electrical properties of the photoresistor and photovoltaic solar cell sensors.

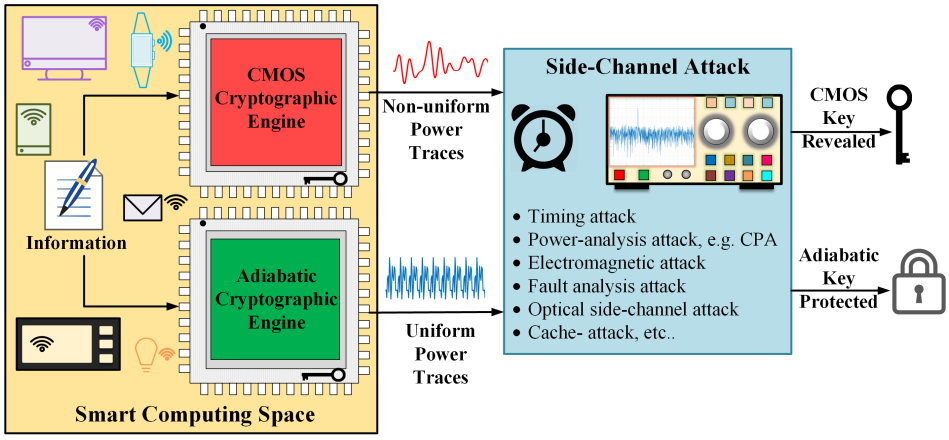

Figure 1.6: Adiabatic logic as a potential solution to design low-power and secure cryptographic circuits.

Another aspect of smart computing device security is to design low-power and secure cryptographic circuits, e.g. block ciphers, stream ciphers. The low-power devices are easy to pray to cyberattacks and can leakage information through a side-channel. Some examples of Side-Channel Attacks (SCA) are timing, power analysis, fault analysis, cache attacks, and electromagnetic radiation attacks. Among different SCA, the power analysis-based attacks are the easiest to implement and popular among attackers. The CMOS-based cryptographic circuits have distinguishable power consumption traces for different operations. A successful Correlation Power Analysis (CPA) attack, a type of SCA, can be carried out to reveal the secret key. The conventional approach to secure cryptographic circuits often results in higher power consumption. It makes them difficult to get adopted in resource-constrained devices. Therefore, designing an energy-efficient and secure cryptographic cipher is an intriguing research direction.

In this dissertation, we explore the energy recovery-based circuit design technique, also known as an adiabatic logic circuit. The adiabatic logic circuit recovers the charge stored in their load capacitor, rather than dissipating it as heat. Further, the adiabatic logic circuit has nearly uniform power traces, unlike the conventional CMOS logic. Therefore, adiabatic logic-based circuit design can disguise the information processed. The proposed energy recovery-based solutions are resilient against CPA attacks and improve the energy consumption requirements.

1.3 Problem Statements and Contribution

In this section, we present the problem definition and key contribution at abstract. The first two problems covered are suitable for the existing sensor-based smart devices. The last two problems address the issue to strengthen the cryptographic circuit against CPA attack, a type of side-channel attack.

1.3.1 TRNG designed using photoresistor sensors

Problem Statement 1:

The True Random Number Generator (TRNG) provides random bits from a physical phenomenon. The random bits are used as seed value in cryptographic key generation circuit, zero-padding, nonce (number only used once) value, salt value bits, initialization vector, and digital signature, etc. The TRNGs are generally designed using transducer or sensors (to convert physical phenomenon in corresponding electrical signal), followed by an amplifier to boost the signal and post-processing algorithm that removes the statistical dependence to generate random bits. In this research problem, we intend to identify a sensor that has electrical properties that can remove the need for external interfacing electronic hardware, and generates quality random bits at a faster speed.

Key Contribution 1:

In this part of the research, we propose the design of a quality random bit generator designed using photoresistor sensors. The photoresistor sensor is widely used in many embedded computing applications, e.g. detecting the change in lighting conditions to activate lights in smart homes and smart street lighting, phototaxic navigation in robotic tadpoles, controlling brightness and contrast in smart televisions, designing heartbeat sensors in smart healthcare, calculating shutter speed in smart cameras, light-activated control circuitry in smart consumer electronics and designing detector for infrared astronomy, infrared spectroscopy and optical coding [49] [50].

- We identified that the electrical properties of the photoresistor sensor are highly suitable for quality random bit generation at a higher rate.

- We proposed a novel additive scrambling process in the post-processing technique suitable in resource-constrained devices. The proposed technique results in a higher random bit generation rate and Shannon entropy value close to 1.
- The proposed TRNG framework does not require external electronic hardware for amplification and interfacing. Thus, the proposed TRNG can be ported on existing photoresistor sensor-based devices easily.

1.3.2 Integrated TRNG-PUF over photovoltaic solar cell sensors

Problem Statement 2:

The Physically Unclonable Function (PUF) is an important hardware security primitives in an embedded computing framework. The PUF can be thought of as analogous to human biometrics. The response of the PUF is used for the device ID, encryption key generation, and secure key storage. The PUF exploits manufacturing variation in device fabrications to generate a static bit pattern. On the other hand, TRNG transforms the random nature of the entropic source (i.e. electrical response of the sensor) into random bits. Therefore, it is very challenging to integrate the fundamentally orthogonal structure of the TRNG and PUF as one unit. In this part of the research, we explored the possibility to unify TRNG and PUF over the sensor-microcontroller interface.

Key Contribution 2:

The photovoltaic (PV) solar cell sensors are the preferred way of harvesting energy in many small computing devices in Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) devices. We explored the electrical response of the PV solar cell to design an integrated TRNG-PUF architecture.

- We propose a novel method histogram-based method to split the response that enables the integration of two architecturally orthogonal primitives, TRNG and PUF around PV solar cells.
- The Iterative Von Neumann post-processing results in an improvement in throughput by approximately 34%.

- The proposed prototype shows promising results for TRNG and PUF responses together.
- The proposed prototype can easily be ported over existing PV solar cell sensor-based devices as there is no need for external hardware for interfacing.

1.3.3 2-Phase Dual-Rail Adiabatic Logic to design secure cryptographic ciphers

Problem Statement 3:

Modern medical devices are collect the physiological information of the patient, communicate to the cloud, and are often battery-powered. Designing energy-efficient and secure cryptographic circuits in low-frequency medical devices are challenging. The adiabatic logic circuits are low-energy solutions and can withstand the CPA attack. In this part of the research, we proposed a novel two-phase sinusoidal clocking implementation called, 2-SPGAL for existing adiabatic logic, Symmetric Pass-Gate Adiabatic Logic (SPGAL).

Key Contribution 3:

The key contribution in this research is summarized as follow:

- This work presents 2-SPGAL, a novel 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL).
- The energy and security of the adiabatic logic largely depend upon the PCG integrated into the design. Therefore, we evaluated the energy efficiency and CPA-resistance of the proposed 2-SPGAL with two different types of synchronous resonant Power Clock Generators (PCGs). Two types of PCGs are 2N2P-PCG and 2N-PCGs.
- The case-study implementation of the cryptographic circuit using proposed 2-SPGAL shows on an average around 50% improvement in energy efficiency compared to CMOS-based counterpart. over the frequency range of 50 kHz to 250 kHz in biomedical device applications.
- The case-study implementation using proposed 2-SPGAL shows on an average approximately 23% improvement in energy consumption compared to another 2-phase adiabatic logic solution, 2-EE-SPFAL [9].

- We demonstrate that the case-study circuit designed using novel 2-SPGAL can successfully defend the encryption key against the CPA attack However, the encryption key is revealed in the same counterpart design using CMOS.

1.3.4 2-Phase Single-Rail Adiabatic Logic to design secure cryptographic ciphers

Problem Statement 4:

The 2-EE-SPFAL and 2-SPGAL produce two outputs at the logic gate, V_{out} and $\overline{V_{out}}$, thus known as, Dual-Rail adiabatic logic. The dual-rail adiabatic logic uses two transistor switching networks to evaluate the logic output. Therefore, it results in higher transistor counts compared to its CMOS counterpart. Reducing the transistor count in Dual-Rail adiabatic logic is necessary for area-constrained portable devices. Further, a reduction in transistor count results in energy-saving design. In this part of the research, we explored a novel single-rail Clocked CMOS Adiabatic Logic (CCAL) to design an energy-efficient and secure cryptographic circuit.

Key Contribution 4:

The key contributions of this work are as follows:

- The CCAL can be an alternate choice for low-energy and CPA-resistant medical devices.
- The case-study implementation saves more than 95% energy for the frequency range 50 kHz to 125 kHz and approximately 60% more energy-saving at 250 kHz compared to its CMOS counterpart. The above energy saving can be highly beneficial to designing low-power cryptographic circuits.
- The case-study implementation shows a significant saving of transistor count compared to dual-rail adiabatic logic 2-EE-SPFAL [9] and 2-SPGAL [10].
- We present the effect of varying tank capacitance in 2N2P-PCG over energy efficiency and security performance.

- The single-rail CCAL based circuitry removes the need for discharge circuitry required in its dual-rail counterpart. It helps to reduce the external need for the control signals for discharge circuitry.
- We demonstrate that the case study designed using CCAL can successfully defend the encryption key against the CPA attack. However, the encryption key is revealed in the same counterpart design using CMOS.

1.4 Thesis Organization

The organization of the report is as follows. Chapter 2 presents the need for security in embedded computing, the role of the hardware security primitives to combat security threats, and their performance evaluation metrics. The first two Chapters are presenting the design of the hardware security primitives designed from sensor-microcontroller interfaces. Chapter 3 presents the proposed prototype of TRNG using photoresistor sensors. In Chapter 4, we explain the novel design to integrate TRNG and PUF over photovoltaic solar cell sensors. The subsequent two chapters present the circuit-designed technology to design energy-efficient and secure cryptographic hardware using adiabatic logic. In chapter 5, we present the novel 2-phase sinusoidal clocking implementation of dual-rail adiabatic logic 2-SPGAL. In Chapter 6, we explored Clocked CMOS Adiabatic Logic (CCAL) to design secure cryptographic circuits with further improvement in energy efficiency and reduction in transistor counts compared to work reported in the previous chapter. Chapter 7 concludes the dissertation report.

The work presented Chapter 3 is published in IEEE conference [51]. Chapter 4 is published in IEEE Consumer Electronic Magazine Journal [52]. The work presented in Chapter 5 is presented as a IEEE conference [10] and currently under review in IEEE Transactions on Consumer Electronics [53]. The work presented in Chapter 6 is currently under review in the IEEE Open Journal of Nanotechnology [54].

Chapter 2

Background and Related Work

The objective of this chapter is to give an idea about the importance of security in smart devices. We also illustrate some of the key security issues and the scope of the research presented in this dissertation report. We discuss the importance of hardware security primitives, TRNG, and PUF. We also discuss the general design of the TRNG and PUF. We also present the background related to the energy recovery logic (i.e. Adiabatic logic). We also illustrate the procedure to carry out Correlation Power Analysis (CPA) attacks without going into deep intense mathematics. The chapter concludes with an explanation of evaluation metrics in hardware security primitives and their potential application listed in the literature.

2.1 Introduction

Over the years, there has been a substantial increment in security attacks on smart devices. The attacker studies the smart device, trying to sort the information based on what may work or may not work, then exploit the vulnerabilities present in heterogeneous connected devices. Further, the IoT devices are easy to attack and typical attacks can be completed within 5 minutes [18]. some of the key vulnerabilities are listed as follow [3]:

- **Eavesdropping:** This is intercepting the communication happening between two IoT devices. The information gathered can be later exploited to plan a bigger attack.

- **Privacy:** The information gathered through eavesdropping can be used to explore unauthorized access.
- **Data-tampering:** The attacker gets unauthorized access and can alter the confidential information happening over the network.
- **Spoofing:** The attacker communicates with the IoT nodes with false identity (impersonating as legitimate). A successful impersonating attack enables the attacker to spoof confidential user information.
- **Code Tempering:** The resource-constrained nodes are relatively easy to pray. The research literature has some examples, in which an attacker can install a malicious patch of the code to affect the performance of the network.
- **Physical availability:** The attacker can alter or damage the sensor or its property. This results in the transfer of an erroneous message from the sensor front end and can hamper the overall function of the system.
- **Denial of Service (DoS):** The DoS and Distributed DoS (DDoS) attack over IoT is getting frequent attention in news. The attacker makes thousands of IoT nodes as "boat" and carries out the DoS/DDoS to halt the operation of a huge network.
- **Accessing restricted part of the network:** The communication infrastructure is consists of several heterogeneous technologies (e.g. Wi-Fi, Bluetooth, ZigBee, etc.) and thus requires gateways. Further, there is no specific communication protocol for IoT devices (e.g. TCP/IP). This results in a back-door to get access to an unauthorized part of the network.
- **Authorization attack:** The attacker gets access to the node without a proper credential and later it can be used for malafide intention. The unavailability of the process to determine the authentication results in an authorization attack.

2.1.1 Background on Key Security Attributes

Cybersecurity is a very broad topic and the basic purpose is to establish the level of trust in the user. A completely secure system should possess the

following properties, viz., confidentiality, integrity, availability, authenticity, and non-repudiation [55]. In this section, we give an abstract idea about the application of TRNG-PUF to maintain the above properties. TRNG and PUF design will be described in detail in the later part of the chapter.

- **Confidentiality:** The objective of this property is to ensure that only intended users have an ineligible message. The messages are encrypted and decrypted using cryptographic algorithms. The IoT nodes are resource-constrained, thus over the years, researchers have proposed lightweight cryptographic algorithms. The cryptographic algorithms are classified in the following categories based on the number of keys: Symmetric (one key) and Asymmetric (use two keys namely: public and private). Data Encryption Standard (DES), Advanced Encryption Standard(AES) [56], Rivest-Shamit-Adleman (RSA) [57], RC2, and RC6 had been traditionally implemented with lower-key size [58]. However, the modern algorithm, e.g. Elliptic Curve Cryptography (ECC) [59, 60] and PRESENT [5] are becoming more popular. The primitives presented in this report, TRNG and PUF can be useful to generate the key for cryptographic algorithms, provide an initialization vector in ciphers.

- **Integrity:** The integrity property guarantees the correctness of the delivered message. Hashing is a common method employed to check that the message is not tempered and altered. The WHIRLPOOL, PHOTON, and Secure Hash Algorithm-3 (SHA-3) family implementation for IoT are examples of hash functions [61, 62]. The input of arbitrary size results in a unique fixed-length output. The Salt bits (generated from TRNG) can be used as an additional input to hash functions to safely store the passwords.

- **Authenticity:** The authenticity validates that the only trusted device be part of the system. The IoT nodes are sometimes deployed into an area where monitoring every physical device is next to impossible. The attacker may forge or temper the sensor or nodes. Authenticity determines that the message is coming from trusted parties. The Privacy-Preserving Mutual Authentication (PPMA) protocols use, both TRNG and PUF responses to mutually authenticate server and IoT node [8]. More detail about PPMA will be explained later in the chapter.

- **Availability:** This is a very crucial property in IoT security. The attackers have used denial of service (DoS) and distributed denial of service (DDoS) flooding attacks on IoT devices to restrict the availability of the system [63].
- **Non-repudiation:** This property ensures that either sender or receiver does not deny any aspect of authenticated communication happened. The successful implementation of this property protects, sender, and receiver from malicious communication intent. One possible way to implement non-repudiation is by introducing Digital Signature (DS). The TRNG bits can be useful as one of the inputs to create DS[64] [44].

2.2 Security: An Overview

The security issues in smart devices are happening at a very rapid pace. Smart connected devices are often a collection of different platforms, technology, communication infrastructure, and physical system. It is challenging to present a unified device architecture that can cover all aspects. The primary objective of this section is to present the security challenges that exist at the device and different layers of the system architecture. The term smart device is a broad umbrella that covers IoT devices, smart healthcare devices, and cyber-physical systems.

2.2.1 Smart Device: A generalized overview

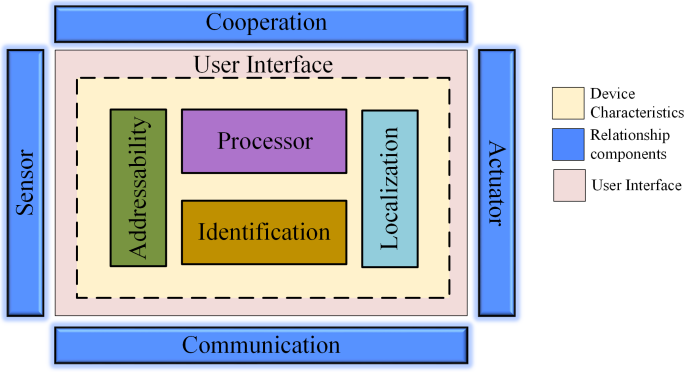

Figure 2.1: Smart device features [3].

In this dissertation, we are restricting our discussion only to resource-constrained devices. The infrastructure in smart connected devices, e.g. IoT, CPS, and smart healthcare devices is almost identical. The IoT devices are widely studied and can serve as a baseline to explain the vulnerabilities in security in such devices. The authors in [3] describe three essential features, viz., specific characteristics, relations between characteristics, and interfaces. The overall idea is represented in Figure 2.1.

Smart Device Characteristics

Processor, addressability, identification, and localization form the important features that set the characteristics of the smart Device.

- The embedded **processor** enables the computational processing based on received inputs and answers to the request coming from the application or internet.
- The important feature of the associating device to address to facilitate its identification and routing of the message via routing is enabled by **addressability.**
- The features that make the unique identity of the device (e.g. MAC address, Unique ID) is the goal of **identifications.**. The PUF can also serve to give unique identification to the device.
- The **localization** enables the device to get related to its actual physical address. The last feature may not be needed in every device. However, this becomes extremely important when the resource-constrained device is implemented in a large geographical area, e.g. agriculture, military, etc.

Relationship between characteristics

The sensor, actuators, cooperation among devices, and network communication technology are the key components in this feature. Their functionality altogether helps interact with the physical world and the Internet.

- **Communication** enables the devices to transmit, and receive the messages over the network. ZigBee, Wi-FI, Bluetooth, Radio Frequency Identification (RFID), and Low-Power Wide Area Networks (LPWANs) are some examples of communication mediums.

- The large set of devices should **cooperate** with other IoT devices for the collective goal of activities and application.
- The **sensor** enables the device to capture the information from the physical environment and provides input to the processor for necessary tasks, and communication to other parts of the network.
- The **actuation** refers to the ability to operate in the surrounding physical environment. This feature completes the application of the task. It is important to note that every device (e.g. fitness trackers) may not have an actuator.

Interface

The interface helps the user to interact with the object, view the information, allow necessary settings, and permit the desired modification based on the inputs. It is important to note that there exists no standardization in interfaces. The interface is usually referred to as the environment created in software. Even though there exist many challenges, we will restrict the discussion only specific to the hardware point of view.

2.2.2 Architecture Layers

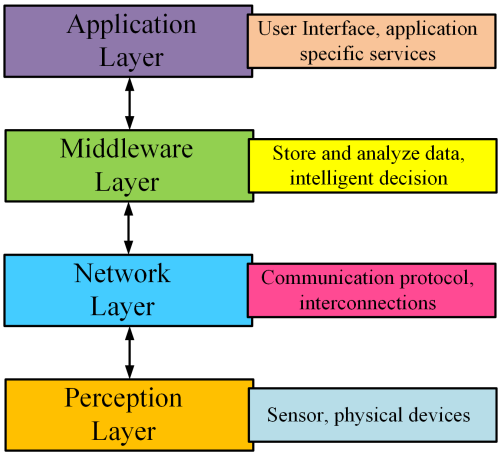

Figure 2.2: Smart Device Architecture layers [4].

There exist many different methodologies to describe the architecture layers (Figure 2.2). There are four layers are, viz., perception, network, middleware, and application. The perception layer uses sensors to collect the information and other constituent hardware parts. The objective of the network layer is to provide communication with other nodes and network components. The layer between, network and application is named the middleware layer. The objective of the middleware layer is to store the data in the cloud, analyze it, and take intelligent decisions. Further, the scalability and inter-operability depend upon an efficient middleware layer. The application layer provides the interface to the user for the intended application.

2.2.3 Security Issues

In this section, we will see some key challenges and issues needed to address security. The classification of security vulnerabilities at different architecture layers will enable us to understand the specific need and likely direction of the research. Table 2.1 lists some of the key IoT security issues and how they can be safeguarded.

Table 2.1: Smart Device Architecture layer security vulnerabilities.

Architecture Layer	**Security Vulnerability**	**Affected security Parameters**
Perception Layer	Device Capturing, Device impersonation, compromises in cryptographic key management	Confidentiality, Integrity, Availability
Network Layer	Spoofing, Altering information, Replaying false routing	Authentication, Integrity
Middleware Layer	malicious code insertion, affecting decision, false multi-party authentication	Confidentiality, Integrity
Application Layer	Creating issues in data access, protection, and retrieval software vulnerabilities attack	Access control, Confidentiality

The perception layer is consists of the sensor, actuators, and their communication infrastructure connecting them to the network layer. The significant issue in the perception layer is to identify between correct and abnormal devices. Attackers can temper, compromise, disable, or destroy the node. These kinds of nodes can be referred to as faulty nodes. We will describe later in the chapter that the output of the PUF can be used to create a unique device identification. Further, key management is a key issue in the perception

layer. It has been demonstrated that storing a local key is susceptible to side-channel attacks. The TRNG and PUF are key components to generate a secure key. The TRNG and PUF presented in this report are designed from sensors and the microcontroller. These features free up the requirement of secure memory storage and make nodes resilient against side-channel attacks.

The network layer carries a large amount of the data, and vulnerabilities can expose to congestion in the network. Authentication and Integrity are the key security concerns at the network layer. The common attacks at the network layer are replay, DoS/DDoS, Man-in-the-Middle (MITM), and malicious code injection. The literature shows the PUF as a promising component in authentication protocols in IoT [65–68].

The middleware layer process the bulk of the data coming from the network layer and takes a decision based on processing. One of the key features of this layer is to filter between valid data and malicious data. Successful cyberattacks can transmit false data, and that can even lead to halt system operations. The application layer provides personalized services. Some key examples of attacks at the application layer are malicious code injection, spear-phishing attacks, cease the device to stop receiving update patches.

2.3 Role of Hardware Security Modules in security framework

2.3.1 True Random Number Generator (TRNG)

Random Number Generators (RNG) are classified as Pseudo-Random Number Generator (PRNG) and True Random Number Generators. The PRNG is also sometimes called Algorithmic and TRNG as Physical due to their underlying mechanism to operate. The key thing in PRNG is to decide the polynomial, which can be based on

- Fibonacci series based polynomial
- Galois LFSR. It is found more efficient compare to its Fibonacci series-based LFSR.

The PRNG is primarily dependent upon maximum length LFSR designed using primitive polynomials. The PRNG response is periodic, and the value

of periodicity depends upon the size of the register. For example, the periodicity of m registers PRNG is 2^{m-1} bit. The word periodicity and sequence length are often used interchangeably in the literature. A single response of m-bits possesses all the necessary properties needed in random numbers. However, they fail collectively.

The algorithms are deterministic in nature. In other words, certain inputs will always result in the same output. The attacker can forcefully reset the operation and can access different input-output combinations. Thereby, it is possible to speculate about the seed value and overall PRNG response. This makes a standalone PRNG response a poor choice in cybersecurity,

High-quality randomness is the utmost requirement in cybersecurity. A true random number generator (TRNG) is a hardware component that generates a string of random bits based on a non-deterministic physical phenomenon as a source of randomness. In recent years many researchers have attempted to use inherent noise in the electronic device, such as Johnson noise, shot noise, Zener noise or random variation in sensor response to design TRNG [44].

The noise source used to generate TRNG bits should possess a high entropy value. The higher entropy from the source results in quality random bits. Low entropic sources are easy to attack. Unlike the ASIC-based TRNG, the sensor-based TRNG can offer the easily perform entropic profile of the noise source. The entropic profile of the random bits can help to speculate the ability of the TRNG to withstand attack.

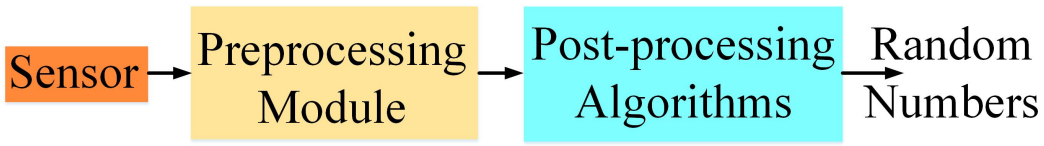

Figure 2.3: General schematic of TRNG (© 2020 IEEE).

TRNG is crucial in many cybersecurity operations, such as asymmetric and symmetric key generation, Digital Signature (DS) creation, initialization vector in the block and stream ciphers, and salt value generation for secure storage. In the existing literature, free-running oscillators (FRO), ASIC, and FPGA-based TRNGs have been explored [44]. Considering the growing importance of the IoT nodes, TRNG designs using existing sensors and microcontrollers have also been explored by researchers in recent times. Figure

2.3 illustrates a generalized design of a sensor-based TRNG.

The existing sensor-based TRNGs have explored sensors, such as accelerometer [69–71], fuel cell [72], hydrogen gas [73], inertial measurement unit (IMU) [74], ECG [75] and RFID [76]. The existing sensor-based TRNGs have a preprocessing module to sample-amplify-filter raw sensor signal [69, 72, 73, 75, 76] or to remove stationery patterns [70] or to add randomness in raw sensor signal[74], before being utilized to extract random bits by post-processing algorithms. The inherent properties of the sensors and preprocessing modules in existing sensors-based TRNG make them suffer from a lower random bit generation rate. For example, the maximum average random bit generation rate in sensors-based TRNG is 250 bps, to the best of our knowledge [71]. As sensors-based TRNG can be designed with minimal redesign costs and minimal performance, area, and power penalties, thereby a faster implementation needs to be developed.

2.3.2 Physically Unclonable Function (PUF)

The PUF was first proposed in [45]. The PUF is a hash function, for a given input resulting in a unique outcome. The PUF uses the minor inherent variation in the device to generate a unique static response. The inherent variations (e.g.jitter, delay) in properties are not controllable and predictable, thus it becomes practically impossible to clone the model. The inputs are commonly referred to as challenges and outcomes as the response. The different inherent variations of each PUF will make different responses to the same challenge.

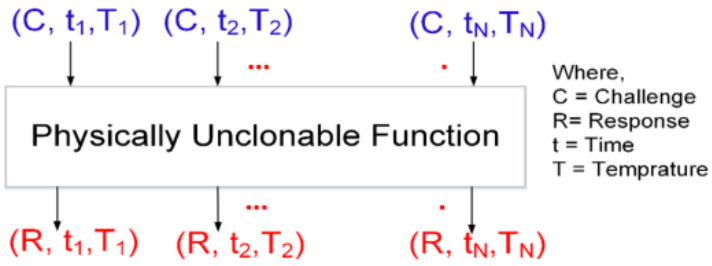

Figure 2.4: Schematic of strong PUF

Physically Unclonable Function (PUF) has emerged as a low-cost tool for hardware authentication and cryptographic key generation. It consists of

two parts: sensor and operational part. The sensor (Optical, Silicon, Coating, LC) part is difficult to clone as no one can match the same underlying manufacturing process variation, which makes it difficult to clone. The operational part generates a response based on the computational algorithm to create a similar or near similar response. The researchers have made the PUF which can be categorized into either Silicon IC-based PUF or Sensor-based PUF. The major advantage of the sensor-based PUF is that it can be designed from the sensors already employed in the system and the testing of the design becomes easier.

There are various methods to design PUFs. In the Ring Oscillator (RO) based PUF, the series connection of the NOT gates is used to generate oscillating output between two voltage levels. As the delay of each gate is not universal and it depends upon the physical process manufacturing variation, the delay will be random, and it can be used to create a unique response for PUF [45] [77].

In the optical PUF, a laser beam is imparted on material doped with a scattered transparent material to generate a speckly or freckled response. This response depends upon the angle of the incident laser wave, doping of the material, and orientation of the material. The laser beam incident at the same angle on different materials will not produce the same output which can be used to generate unique response [45] [77].

The LC PUF, e.g. Piezo, has a coil and a capacitance from the metallic body, which is not unique due to process variation in the manufacturing of each sensor. This results into different resonance frequency which can be used as unique identifier for each sensor [45] [77]. PUFs are categorized into two subgroups:

- **Strong PUF:** It has a large set of challenge-response pairs. This is a critical property in device authentication.
- **Weak PUF:** Only generates unique signature bits. Used to give seed bits for cryptographic key generation

The natural variation in the manufacturing procedure makes PUF, an alluring choice in many security applications. It would be only possible to attack the system if the attacker or adversary gets the actual PUF being implemented. Many attempts have been made to incorporate PUF into a variety of applications such as key storage, unique device id generation, and

to check the authenticity of the hardware connected in the network. To detect the malicious insertion of the hardware, the scheme that is employed is that during the initial booting process every sensor puts its signature to verify its identity.

The response of the PUF can be used in cryptographic algorithms to generate the secret key which is not required to be stored in secure memory. This can lead to the removal of costly secure memory storage as a secure key derived from the response of the PUF itself. Further, the uniqueness of the PUF properties makes challenges useless without having access to the actual PUF.

It is proposed by M. Feiri, J. petit, F. kargl et al. in [78] that PUF can be easily incorporated into IoT security infrastructure. It has been demonstrated in [79] by authors that PUF can also be useful to prevent Denial of Service (DoS) attacks. This requires authentication from the central monitor to authenticate any IoT node to communicate.

2.3.3 PRESENT: Lightweight Cryptographic Cipher

The objective of this section is to illustrate the importance of the Lightweight cryptographic cipher in resource-constrained devices. In this research, we have selected PRESENT, a lightweight cryptographic cipher for case-study implementation. The case-study implementation of the PRESENT designed using adiabatic logic is compared for energy efficiency and security performance with its baseline counterpart designed using conventional CMOS logic. We explain the background information about the PRESENT algorithm later in this section.

Background on Lightweight Cryptographic Ciphers

The emerging applications, e.g. IoT, Cyber-Physical Systems, distributed control systems, sensor networks, and health care devices, have many battery-operated and wirelessly connected devices. These devices operate in incoherence to accomplish certain functions. The previously proposed cryptographic solutions for desktop or server environments are not suitable for such area-constrained devices. The National Institute of Standards and Technology recognized the need for Lightweight Cryptography (LWC) [80].

The cryptographic algorithms are divided in two categories. First, Asymmetric cryptography (also known as public-private key cryptography), which

is used primarily in secure-key exchange, digital signature, etc. Second, symmetric-key cryptography, which finds application in encryption and decryption of bulk data. Symmetric key cryptography is also referred sometimes to as secret key cryptography as both sender and receiver use a common key. The processing operations in symmetric key cryptography mostly involve XORing and permutations. The symmetric key cryptographic algorithms are further classified in Block ciphers and stream ciphers.

Stream cipher uses the same key length as data block size and encrypts a single bit at a time. A few commonly used lightweight stream ciphers are Espresso, Chacha, eStream, Trivium, Grain 128, and WG-8. The stream ciphers have a longer setup time, and their throughput is lower. The current research literature on stream ciphers do not provide significant advantages for their implementation in resource-constrained devices [81] [82] [83].

On the other hand, block cipher operates on a fixed size of data blocks and round-key derived from the stored secret key. In research literature, Block ciphers have been shown as as one of the block (other two are PRNG and hash function) to build challenge-response protocol based secure identification system [5] [84] [85] [86] [87] [88]. Further, the block cipher has relatively higher throughput and fewer area requirements compared to stream cipher in resource-constrained hardware. HIGHT, mCrypton, SEA (Scalable Encryption Algorithm), TEA (Tiny Encryption Algorithm), KATAN, and PRESENT are some examples of the block ciphers [83] [89]. We selected the PRESENT as a case-study implementation for the following reasons.

- The authors in [83] [89] have shown that the throughput and area-requirement are optimum in PRESENT implementation compared to other block ciphers.
- PRESENT has a simple architecture, and better security [5]. This makes it a suitable candidate for security applications in resource-constrained devices.
- Beside the encryption process, the PRESENT can be used for authentication within challenge-response protocols [89] [90].

PRESENT encryption algorithm

```
generateRoundKeys()
for i = 1 to 31 do

    addRoundKey(STATE, Ki)
    S-BOXLayer(STATE)
    P-LAYER(STATE)

end for
addRoundKey(STATE, K32)
```

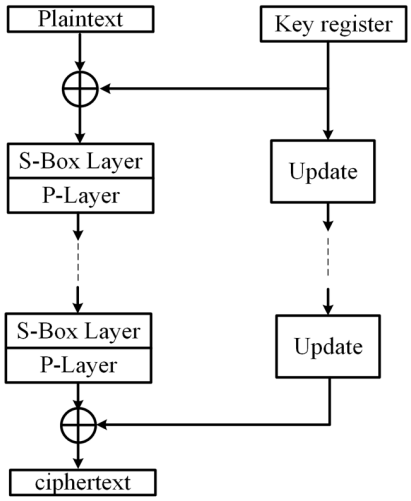

Figure 2.5: Top level description of PRESENT encryption scheme [5].

The PRESENT block cipher consists of identical 31 rounds of the operations. The data block length is 64 bit and the key length comes in two variants of 80-bit and 128-bit. Based on the key length, there are two different versions, PRESENT-80 and PRESENT-120. Figure 2.5 shows the top-level algorithmic description of the PRESENT algorithm. Each of the 31 rounds has three primary operations, summarized below [5].

1. **addRoundKey:** Out of 80-bit of the key, 64-bit is derived and XORed with the 64-bit of the plaintext data block.

2. **S-BoxLayer:** The Substitution-Box (S-Box) takes a 4-bit input and does the non-linear transformation to generate 4-bit output. There is a total of 16 identical S-Box are required to implement one round of PRESENT encryption.

3. **P-Layer:** The Permutation-Layer (P-Layer) is a bit permutation on the output of the S-Box. The P-layer can be implemented in hardware by aliasing the wires. There is not a requirement of any processing elements, e.g. transistor.

The decryption process in PRESENT is achieved by performing the above operation in reverse order. Considering the simple hardware design, better throughput, improved security, and suitability for the resource-constrained devices, we decided to implement PRESENT-80 one round of encryption circuits as a case-study implementation. In subsequent chapters, we show an apple to apple comparison between proposed adiabatic logic-based and CMOS logic-based implementation for energy-efficiency and security performance comparison.

2.4 Adiabatic Circuits to design Energy Efficient and CPA Secure Cryptographic Ciphers

The countermeasure against power analysis attacks (e.g. CPA attack) can be classified as masking [91], random instruction injection [92], non-deterministic processors [93], random register renaming [94], secure co-processors [95], and cell-level countermeasures [96]. In cell-level countermeasure, e.g. adiabatic logic, the focus is on designing logic gates with uniform power traces. Further, the charge recovery operation makes adiabatic logic an attractive design choice for energy-efficient and CPA-resistant IMDs. The objective of this section is to give the background adiabatic logic. Additionally, the commonly used metrics in literature to evaluate the security of the cryptographic hardware are discussed.

2.4.1 Adiabatic logic

To reduce the energy consumption, the adiabatic logic design technique recycles the energy stored in capacitive load back to the power clock circuit. The capacitive load is charged using the constant current source, rather than the conventional approach to use the constant voltage [97]. The constant current source is practically achieved by a ramp referred to as a power clock. The generalized switching model, charging and the discharging path of the adiabatic logic is shown in Figure 2.6.

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

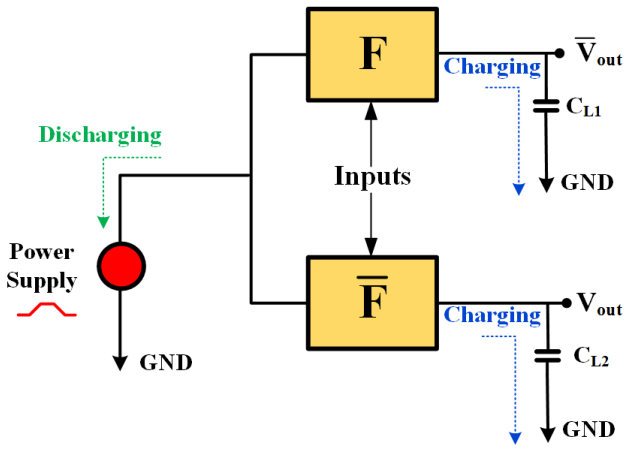

Figure 2.6: Charging and discharging in adiabatic circuits [6] (© 2020 IEEE).

Equation 2.1 shows the energy consumption in adiabatic logic circuits. In equation 1, T is charging or discharging time-period, load capacitor C, adiabatic logic-based circuit resistance R, and V_{dd} is the full-swing voltage of power clocking signal. Equation 1 helps to understand that adiabatic circuitry has significantly low energy consumption for low-frequency operations compared to standard CMOS.

2.5 Sinusoidal Power Clock Generator for 2-Phase adiabatic circuits

The adiabatic logic systems consist of primarily two main components. First, the adiabatic circuit was designed using adiabatic logic cells. The second, the Power Clock Generator (PCG) circuit. The PCG supplies the power clock for adiabatic circuit operation, and the stored charge is recovered back to PCG. The poor design of the PCG can result in non-efficient adiabatic operation and less energy saving. Therefore, the energy and CPA resilient capability of the adiabatic system needs to be evaluated with PCGs integrated with the design.

The PCGs are broadly classified in step-wise charging PCG and resonant clock generators. The oscillator-based resonant generator can recover the charge stored in the load capacitor back to the inductor. Further, the higher power conversion efficiency makes it more suitable for the adiabatic logic

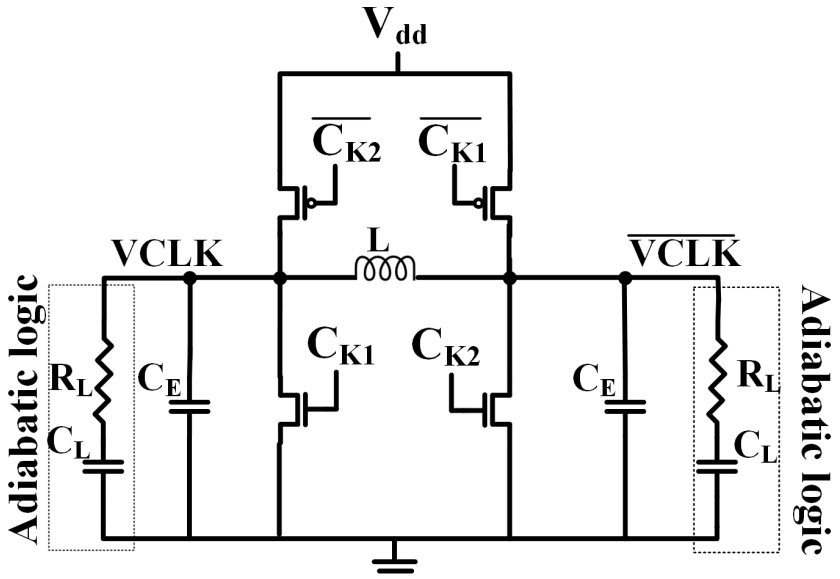

Figure 2.7: 2N2P-PCG [7].

operation. The synchronous resonant are found to be more energy-efficient, and its example includes 2N-PCG and 2N2P-PCG [7]. The circuit diagram for 2N-PCG and 2N2P-PCG is shown in Figure 2.7 and Figure ref2N-PCG respectively. The 2N-PCG has two NMOS transistors, hence, referred to as 2N-PCG. The two inductors of the same value are interfaced with dc voltage equal to half of the full-swing voltage required. Similarly, 2N2P-PCG has two PMOS and two NMOS transistors. 2N2P-PCG requires only one inductor, and dc supply equal to full-swing voltage.

The schematic to interface the proposed adiabatic logic-based circuitry with synchronous PCGs is shown in Figure **??**. The synchronous resonant PCG uses an external time-base signal. The external time-base signal allows adiabatic circuitry to synchronous with other non-adiabatic circuits in a larger system. The differential operation of the adiabatic logic makes the lumped capacitance value independent of the frequency of the operation. Thus, the change of frequency operation can be achieved by varying the external inductor value.

$$f_0 = \frac{1}{2\pi\sqrt{L\left(\frac{C}{2}\right)}} \tag{2.2}$$

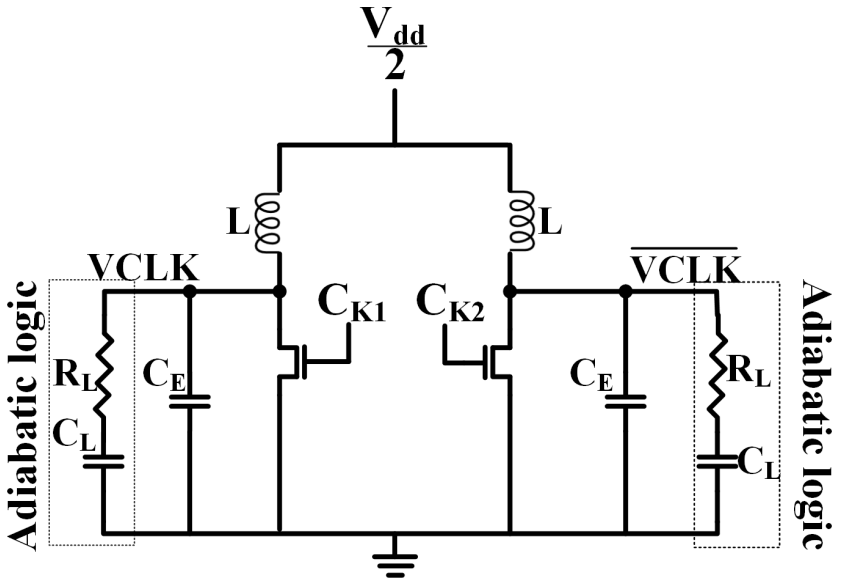

Figure 2.8: 2N-PCG [7].

The 2N2P-PCG requires four external time-base signals. The external time-base signals can help to synchronize the adiabatic circuits in larger conventional non-adiabatic circuits. Figure 2.10 shows the external time-base control signals used to operate 2N2P-PCG. The 2N2P-PCG generates two out-of-phase signals by two identical circuits operating in a lock-step manner. The operation frequency of the 2N2P-PCG is given by Equation 2.2. CCAL logic requires two out-of-phase sinusoidal power-clock signals, VPC and $\overline{VPC}$. Figure 2.9 shows the interfacing of 2N2P-PCG with the adiabatic logic circuits.

The timing diagram of the external control signal is shown in Figure 2.10. The two external control signals CK_1 and CK_2 are out-of-phase with each other.

2.6 Background on Correlation Power Analysis (CPA) Attack

The recent growing concern on devise security has made the researcher to focus on exploring both possible attack and defensive strategies. To build

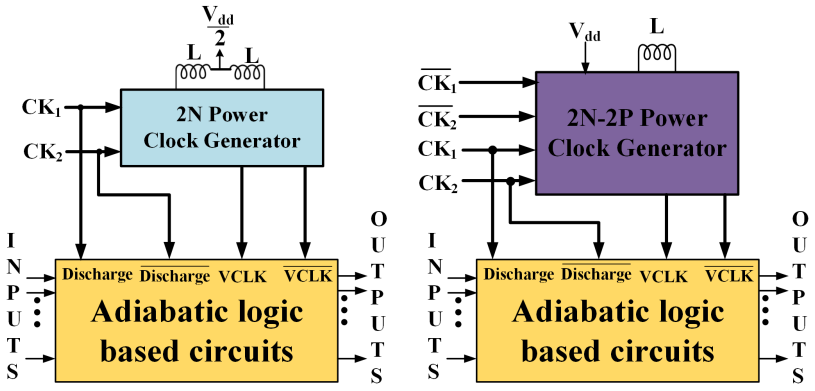

Figure 2.9: PCG interfacing with adiabatic logic circuits.

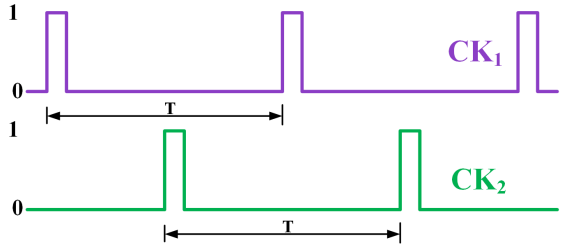

Figure 2.10: Control signals in 2-Phase PCG design [7].

a suitable defensive policy, it becomes important to understand potential vulnerabilities and exploitation. Side-Channel Attacks (SCA) is one such growing concern that compromises device security. In this section, we present background information on SCA. For the scope of the research presented in this dissertation report, we illustrate power analysis-based SCA later in this section.

2.6.1 Side Channel Attack

Implementing the cryptographic algorithm in hardware lead to side-channel attacks. The primary objective of the Side-Channel Attack (SCA) is to reveal the secret key used in the cryptographic circuit. SCA hypothesizes that the physical output of cryptographic circuits, e.g. heat, power consumption, electromagnetic radiations, timing to carry out particular operations correlate with the internal state of the cryptographic circuit.

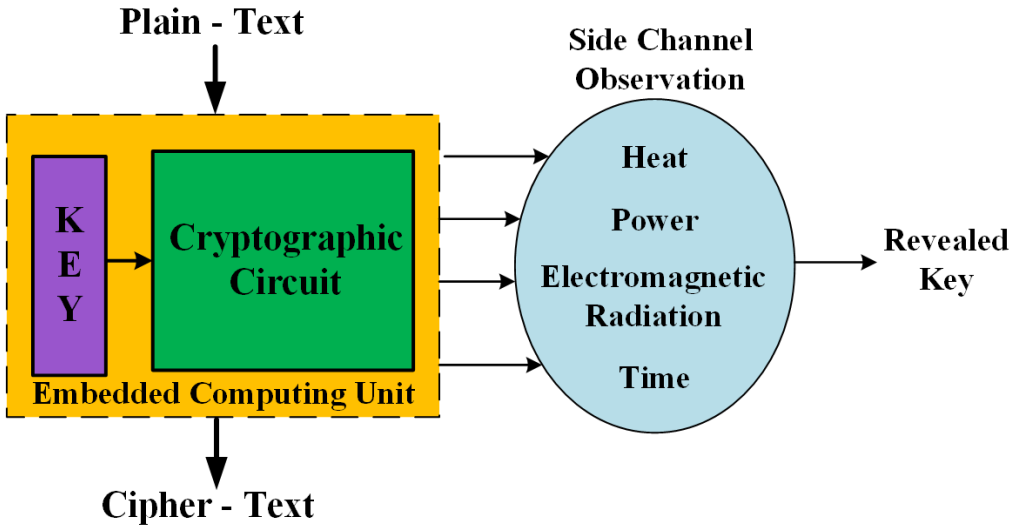

Figure 2.11: Side-Channel Attack.

Figure 2.11 demonstrates the concept of the SCA at abstract. The researcher in [98] described 10 different possible SCAs. Among them, the timing analysis attacks [99], fault attacks [100] and power analysis attacks [101], [91] are commonly employed. Further, the power analysis attack is very simple to implement, less costly and found more lethal to reveal the key used

in the cryptographic circuit. Any novice programmer with simple knowledge of electrical wiring can easily carry out a power analysis attack. They have become the first choice of many attackers in recent times. Therefore, we focused primarily on defending the cryptographic circuit against power analysis attacks.

The power analysis attacks are performed by observing the power consumption traces of cryptographic devices. There are three main power analysis attacks: Simple Power Analysis (SPA) attacks, Differential Power Analysis (DPA) attacks, and Correlation Power Analysis (CPA) attacks. In each power analysis attack, the power traces are collected from the cryptographic device during the data-encryption process being carried out.

In SPA, the collected power traces (or current) are graphically interpreted over a period of time. The DPA is the next evaluation in the power analysis attack after SPA. DPA computes the difference of the mean (thus called the difference of means power attack by some researchers). If the difference comes out to be zero, then two power traces are not correlated. If the two power traces are correlated then the difference will be a non-zero value. The larger number of traces results in two advantages. First, the smaller correlation can become apparent with time as trace size becomes larger. Second, the noise gets effectively canceled out in the subtraction process.

The DPA suffers the problem of the ghost peaks, i.e. some peaks in correlation value occur for the wrong guesses. Sometimes, they appear larger than the actual key value, thus resulting in a wrong key guess. The practical problems associated with ghost peaks are explained in detail in article [102]. On the other hand, CPA requires fewer traces. DPA on average needs 30% more power traces compared to CPA. Therefore, we used the CPA attack to measure the vulnerability of the designed cryptographic circuit.

2.6.2 Procedure to Carryout Correlation Power Analysis (CPA) Attack

The procedure to perform the CPA and DPA can be explained in three steps. Out of which the first two steps are exactly similar, and they differ only at the last step. Algorithm 1 describes the CPA process. In CPA, the assumption is that the attacker knows the cryptographic algorithm, however, the electronic circuit that performs the cryptographic process is unknown. The objective of the CPA is to reveal the encryption key used in the cryptographic circuit.

The procedure to perform the CPA is described below.

Algorithm 1 Correlation Power Analysis (CPA) attack.

1: $T = (T_1, T_2, \ldots, T_N) \leftarrow$ Known Plain-Text
2: $E\ [\ ] \leftarrow$ Every Possible Encryption for known Plain-Text
3: $HW_i\ [\ ] \leftarrow$ Hamming Weight
4: $\rho_k \leftarrow$ Correlation Coefficient
Perform Cryptographic Circuit Power Traces Collection Procedure
5: $\{P_i^1 \mid i = 1, 2, \ldots, N\} \leftarrow$ Power Traces for each T
6: **for** each key, $k_j \in \{0, 1, \ldots, 2^n\}$ **do**
7: Calculate $E\ [\ ] = S - Box(T_1^j \oplus k_j)$
8: $\{HW_j\,(x_1) \mid j = 1, 2, \ldots, N\} = Hamming\ Weight(E[\ ])$
9: $\rho =$ Pearson Coefficient (HW_i, P_i)
10: **return** Best Candidate $= arg\ max\ \rho$

1. The attacker prepares the known plain-text inputs (T) of size N. Collect the power traces (P) from the device under attack for each plain-text input. The power traces (or current traces) can be obtained at the power supply terminal and "real-value" load device, e.g. oscilloscope.

2. The attacker prepares the hypothetical power model. First, for each known plain-text is encrypted using all possible key-value $E = S - Box(T_j^1 \oplus k_j)$. The S-Box does a non-linear transformation of the ciphertext. The S-Box transformation is known in the public domain as a part of the cryptographic algorithm. Second, the attacker calculates the Hamming Weight (HW), i.e. number of non-zero bits, for each encrypted output.

$$\rho(HW, P) = \frac{\mathrm{Cov}(HW, P)}{\sqrt{\mathrm{Var}(HW)}\sqrt{\mathrm{Var}(P)}} \tag{2.3}$$

$$\rho(HW, P) = \frac{\sum_{i=1}^{N}\left(HW_i - \overline{HW}\right)\left(P_i - \overline{P}\right)}{\sqrt{\sum_{i=1}^{N}\left(HW_i - \overline{HW}\right)^2}\sqrt{\sum_{i-1}^{N}\left(P_i - \overline{P}\right)^2}} \tag{2.4}$$

3. The attacker performs the correlation procedure between the hypothetical power model developed (step 2) and collected power-traces (step

1). The best key candidate is speculated for the correlation matrix ($\rho(HW, P)$) that has the highest absolute sum value. The CPA uses Pearson Coefficient (Equation 2.4) to calculate correlation value.

2.7 Performance Metrics for Hardware Security Primitives

The TRNG and PUF are fundamentally different in design, and their usage. Thereby, the evaluation criteria are different. This section explains the performance metrics to evaluate the TRNG and PUF. Further, we also explain the performance metrics to evaluate the energy efficiency and security performance of the adiabatic circuits.

2.7.1 TRNG Performance Metrics

The randomness of the TRNG is evaluated by the various test suite, such as Diehard, National Institute of Standards and Technology (NIST), TESTU01, and FIPS 140-2. The Statistical Test Suite (STS) created by NIST is a comprehensive report taking a gander at different parts of arbitrariness in a long succession of bits. It was developed after DES was proven to be hackable. It is a significant apparatus to figure out the randomness of the TRNGs.

15 different statistical tests are evaluated. Every test is based on the calculation of chi-square variation (χ^2) to calculate the p-Value. Table 2.2 summarizes the objective of each test in NIST STS.

2.7.2 PUF Performance Metrics

Reliability

This parameter is the measure of how likely the PUF will be able to produce the same response at a different time and under different external conditions.

$$\text{Reliability} = 100\% - \frac{1}{k}\sum_{i=1}^{k}\frac{HD\left(R_i, R'_{i,t}\right)}{n} \tag{2.5}$$

Table 2.2: Objective of different tests in NIST Statistical Test Suit

Test Number	Test Name	Purpose
1	Frequency	To find Proportion of 1s and 0s
2	Frequency Test within Block	To find proportion of 1s and 0s within a block in given sequence
3	Runs	To find the total number of uninterrupted sequence of bits
4	Longest runs of 1s and 0s	To find longest run within a block in given sequence
5	Binary Matrix Run	To find the linear dependence in fixed length sub-strings to original string of bits or sequence
6	Fourier Transform	To detect the periodic feature in given sequence
7	Non-Overlapping Template	To find the prespecified target sequences in the given block. If the pattern is not found then the test window is incremented by 1 bit
8	Overlapping Template	To find the occurrence of prespecified target bit patterns
9	Maurer's Universal statistic	To find the number of bits in two matched sequences
10	Linear complexity	It is based on Linear Feedback Shift Register (LFSR). The generated sequence should have same complexity as LFSR
11	Serial	To find the frequency of all possible overlapping sequence
12	Approximate Entropy	It compares the frequency of two consecutive length overlapping sequence with expected result
13	Cumulative	To check that cumulative sum of sequence is too large or small
14	Random Excursion	To find the visit of cumulative sum within cycle is as per random sequence is as per random sequence
15	Random Excursion Variant	To find the number deviation in expected visit to sequence from various random walks

In equation 2.1, the $HD\left(R_i, R'_{i,t}\right)$ is Hamming Distance (HD) between the reference response R_i and the instantaneous PUF response, $R'_{i,t}$. Further, k represents different number of PUF instances created. The ideal value of the PUF Reliability should be 100%.

Uniformity

The metric uniformity tells that how much balance the response of the PUF is. This is an indication that the generated response should have the same number of ones and zeros in the response bit pattern. The following equation

defines uniformity.

$$\text{Uniformity } = \frac{1}{n}\sum_{i=1}^{n} R_{i,l} * 100\% \tag{2.6}$$

Where, $R_{i,l}$ represents the i^{th} bit of a n-bit response generated by PUF.

Uniqueness

Uniqueness metric indicates how well the copy of the PUF is unique to its own and different from other copies of the same PUF design. It requires a large number of PUF copies to evaluate the criteria.

2.7.3 Energy-Efficiency and Security Performance Metrics in Adiabatic Circuits

The CPA has proven its success, and its widely used by malicious cyber attackers against, both asymmetric and symmetric cryptographic algorithms [102]. The adiabatic logic maintains the uniform current traces. The benefit of the adiabatic logic should be evaluated by its ability to withstand the CPA. The common metric used to check the robustness of the hardware against CPA are Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) [6] [103] [104] [105] [106] [107].

$$NED = \frac{(E_{\max} - E_{\min})}{E_{\max}} \tag{2.7}$$

$$NSD = \frac{\sigma}{E_{avg}} = \frac{1}{E_{avg}}\sqrt{\sum_{k=1}^{N} \frac{(E_i - E_{avg})^2}{N}} \tag{2.8}$$

The NED value is the difference between the maximum and minimum energy consumption for all possible input combinations. NSD is the deviation of the instantaneous energy to the average energy consumption. Lower NED and NSD value show that the hardware is less exploitable to the CPA. For the success of the CPA attack, the hypothetical power model (calculated based on hamming weight) should be linearly proportional to actual side-channel leakages. Thus, less deviation in power traces makes it difficult to reveal the encryption keys.

2.8 Application of Hardware Security Primitives

In this section, we will see the usefulness of TRNG and PUF in different cryptographic operations. The researchers in [44, 108, 109] have described the role of the TRNG and PUF in IoT security.

2.8.1 Cryptographic operations

Traditionally, a secure memory is used to store the secret key. However, it has been shown by researchers that this memory is not resilient against cyber attacks. Key generation using TRNG and PUF is one of the most common applications in IoT. Having either PUF or TRNG can remove the requirement of the key generation. The advantage of the PUF is that it is impossible to clone them. The response of the TRNG is unpredictable, and hence the usage of it in key generation makes it practically impossible to speculate the key.

If the TRNG has passed the NIST-STS testing then it guarantees there exists enough randomness in TRNG response [110, 111]. A high entropic response of the TRNG is a suitable candidate to be used as a key in symmetric encryption. However, in reality, the response of the TRNG bits can always be checked that it satisfies certain properties for the key as needed in symmetric or asymmetric cryptographic algorithm [71]. The researchers in [112] provided detail explanation for various Key-Derivation Function (KDF). The scheme uses an approach called the extract-then-expand approach. It consists of two modules, randomness extractor (TRNG) and Pseudo-Random Function (PRF) generator. The TRNG bits are used as seed bits, which later are expanded by PRF. Further, the response from the TRNG can be used as an initialization vector in a cryptographic cipher. The TRNG bits are the preferred direction to be used as salt bits, padding bits in hashing [44].

The PUFs are the most preferred way to replace the secure key generation mechanism, secure key storage keys, and their management. The PUF response is used as a seed to the circuit which can generate the key every time it is needed. This frees up the requirement of secret storage. The secure memory is costly and slower in the speed of operations. The uniqueness property of the PUF allows storing the challenge in insecure memory. Though,

challenges may be known, however as every PUF responds differently. Thus, the response of every PUF used to derive the key will be different.

2.8.2 Usage of the PUF for Authentication

The PUF can provide unique identification among the many IoT devices connected. The traditional authentication scheme works mostly based on providing credentials, e.g. passwords, digital certificates, etc. The password-based mechanism is not suitable in IoT. Many IoT devices can cause the issue of password dependency, and it's very challenging to bind access to the request coming from a particular IoT device. Further, the authentication protocol needs to be lightweight. Over the years many lightweight authentication protocols on PUF based authentication are proposed [113–122]. The PUF is a promising candidate that works on the challenge-response pair mechanism, however, it still requires storing the challenge-response pair at the verifier end. The researcher in [65] has proposed the scheme which blends the usage of PUF with Identity Based Encryption (IBE) for authentication. The proposed scheme in [65] is found resilient against synchronization attack, replay attack, token-server impersonating, and Dos/DDoS.

2.8.3 Privacy Preserving Mutual Authentication (PPMA)

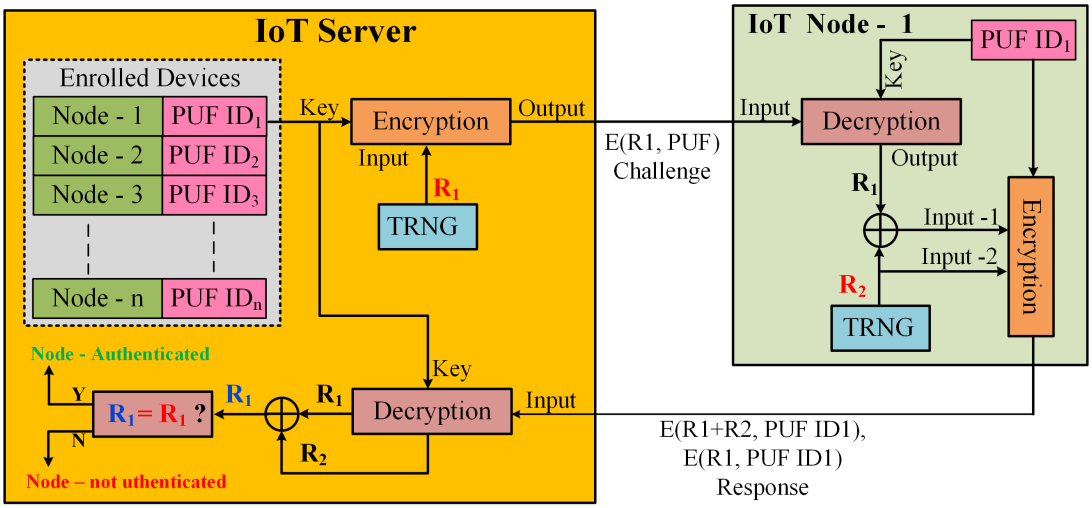

Figure 2.12: PPMA model [8]

The Privacy-Preserving Mutual Authentication (PPMA) uses a repeated challenge-response mechanism. It requires the presence of the TRNG and PUF together. The objective of the scheme is to authenticate the IoT device. It is assumed that the PUF id of the node is communicated to the server earlier via a secret channel. The R1, R2 are the two random numbers and PUF^i represents the unique id generated using PUF. The scheme is explained in following steps [123] [8].

1. The server encrypts the random number (R1) using the PUF ID of the IoT device to be authenticated. The encrypted R1 is passed as a challenge to the IoT node.

2. The IoT devices decrypt the challenge and get the R1. The R1 is added with a new random number (R2) from the TRNG of the node.

3. The IoT node creates two encrypted copies using PUF ID for random numbers R2 and R1+R2. The encrypted message is sent back to the server.

4. The server recovers the two encryption message, and successively derive the original R1. If the received and transmitted copies of R1 are the same then the IoT device is authenticated.

It is important to note that we are not transmitting the PUF ID directly. The key advantage of the PPMA is that, though eavesdroppers can listen to the encrypted message, however, it will be not intelligible. Further, the symmetrical usage of R1 and R2 enables the mutual authentication of server and IoT devices. The addition of R1 with a local copy of R2 ensures the receiver that even if the R1 would not have sufficient entropy, however, its PUF ID is encrypted with full entropy (R1+R2). Also, the IoT node sending the two digital signatures (encrypted with R2 and R1+R2) can limit the scope for an attacker to rely on multiple traces with a common secret key. Thus, in PPMA, the attacker is limited to having access only to the encrypted copy of the message [123] [8].

The PUF produces the static bit response, and TRNG produces dynamic bit responses from the same entropy source. Hence, the design of TRNG and PUF is orthogonal. The architecture proposed in Chapter 4 can be suitable for the PPMA scheme.

Chapter 3

Design of True Random Number Generator (TRNG) from photoresistor Sensor

True Random Number Generator (TRNG) is an essential hardware security primitives. TRNG can be thought of as a mathematical function that samples some source of randomness (e.g. noise, variation in the electrical response of the device due to manufacturing variation). Designing the TRNG from randomness present in the electrical response of the sensor is a novel research direction.

The research work presented in this chapter was previously published in [51] as A. Degada and H. Thapliyal, "Harnessing uncertainty in photoresistor sensor for true random number generation in iot devices," in 2020 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-5,

3.1 Introduction

In this chapter, we propose a True Random Number Generator (TRNG) design that is designed by exploring randomness present in the electrical response of the photoresistor sensor. The true random bits generated from the TRNG can be used directly as zero-padding, nonce (number only used once) value, salt value bits, initialization vector, and digital signature, etc. The encryption key generation from TRNGs are carried out in two different ways

[124]. First, for lightweight cryptographic cipher (the key size is typically less than 128 bits), the output from TRNGs can be used directly [125]. Secondly, for the conventional cryptographic algorithms, the true-random bits can be used as seed value in cryptographic key generation algorithms to generate key of larger size (e.g. 2048 bits, 4096 bits) [124] [126] [127].

The photoresistor sensor is widely used in many embedded computing applications, e.g. detecting the change in lighting conditions to activate lights in smart homes and smart street lighting, phototaxic navigation in robotic tadpoles, controlling brightness and contrast in smart televisions, designing heartbeat sensors in smart healthcare, calculating shutter speed in smart cameras, light-activated control circuitry in smart consumer electronics and designing detector for infrared astronomy, infrared spectroscopy, and optical coding. The proposed design is constructed from components that are common in smart computing devices such as microcontrollers and existing photoresistor sensors.

In this chapter, we first illustrate the evaluation and photoresistor sensor as a source of randomness. It is followed by a discussion on the hardware and software setup of the proposed TRNG prototype. The TRNG response bit performance and discussion are followed subsequently. Lastly, we summarized the important contribution.

3.2 Evaluation of Randomness in Photoresistor Sensor

A practical Analog to Digital Converter (ADC) in a microcontroller has Root Mean Square (RMS), quantization, and code-transition noise. Our software framework does not involve any steps to remove such ADC noises. Thereby, we hypothesized that voltage across a photoresistor sensor sampled by microcontroller ADC can result in variations across some of the least significant bits (LSBs). The variation in LSBs due to slow response time, nonlinear characteristic, and ADC noise serve as a practical proof of randomness.

To evaluate randomness, we set up (as shown in Figure 3.2) a voltage divider circuit using a photoresistor sensor and 10 kΩ resistor connected between supply and ground voltage of a microcontroller(Tiva^{TM} C series TM4C123GH6PM in our setup). The ADC of the microcontroller was configured to sample the change in voltage across the photoresistor sensor and

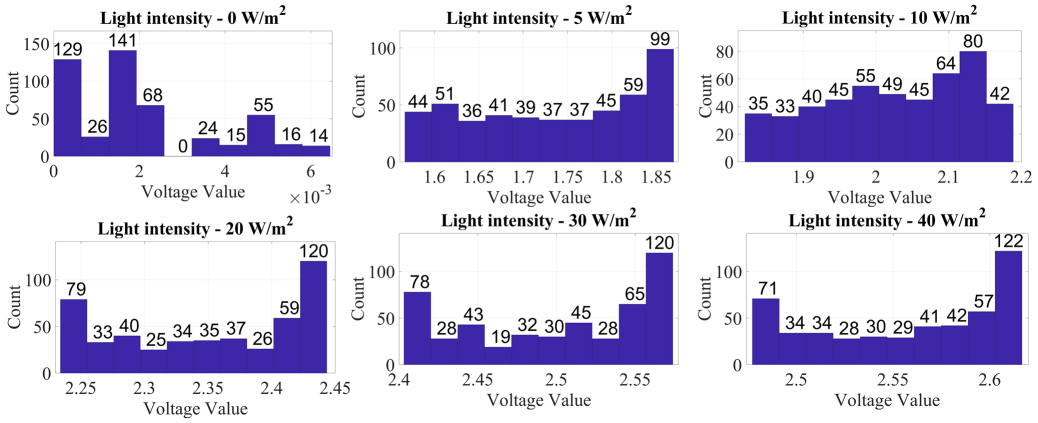

Figure 3.1: Histogram of photoresistor sensor voltage at different light intensity (© 2020 IEEE).

supply voltage. The setup was placed inside a light chamber that facilitates change in light intensity from 0 W/m^2 (Extreme Dark) to 40 W/m^2 (Normal Surrounding light). Figure 3.1 shows the histogram of 488 voltage readings across a photoresistor sensor. It can be observed from Figure 3.1 that the histogram has near-uniform voltage distribution (over $\approx$ 200 mv range) at every light except for a slightly skewed distribution at 0 W/m^2(extreme dark). Hence, the photoresistor sensor has a prospect to work as a source of randomness. The technique to mitigate close distribution of photoresistor voltage at 0 W/m^2 is explained later in this chapter.

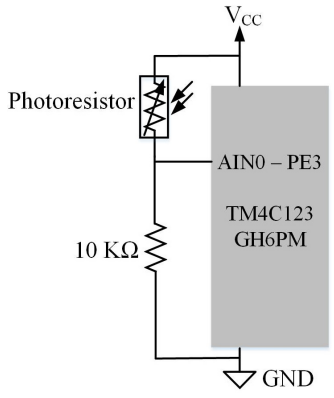

Figure 3.2: Photoresistor-microcontroller Setup to study histogram of sampled voltage (© 2020 IEEE).

3.3 Architecture of Photoresistor based TRNG

In this section, we evaluate the uncertainty of photoresistor as a measure of randomness and explain the electronic hardware and software framework for proposed TRNG. We assume that the microcontroller's CPU operation and its memory are resilient against attack.

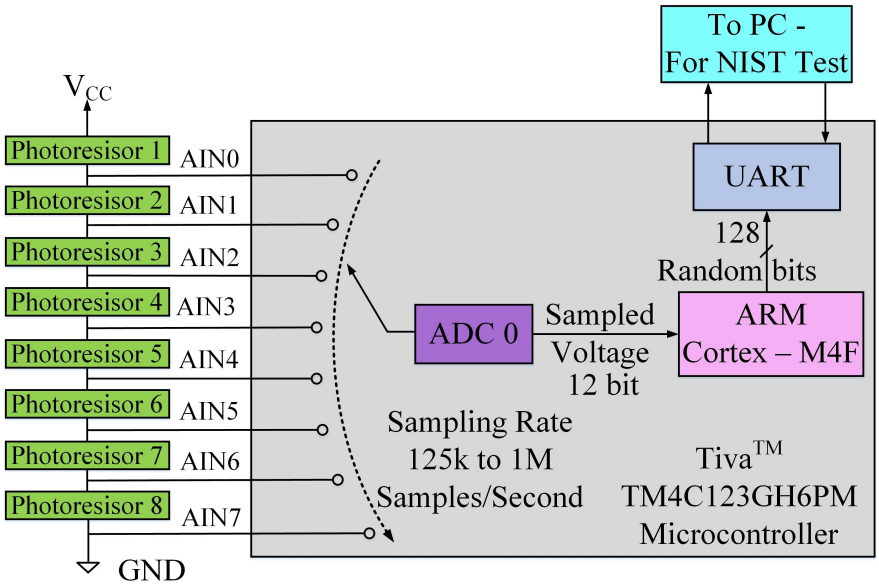

Figure 3.3: Hardware setup of proposed TRNG (© 2020 IEEE).

3.3.1 Electronic Hardware

The electronic hardware of the proposed TRNG is shown in Figure 3.3. It has eight photoresistor sensors connected with the ADC pins of an ARM Cortex-M4 microcontroller (we implemented a prototype using PDV-P8104 photoresistor and Tiva™ C series TM4C123GH6PM microcontroller). The photoresistor sensors in IoT nodes are usually configured in arrays and manufacturing process variation causes each sensor to respond differently, even at the same ambient light condition. This results in more uncertainty and can help to achieve a faster random bit generation rate. The interfacing to PC is done via Universal Asynchronous Receiver-Transmitter (UART) to transmit random bits for NIST STS testing. The UART interfacing can be omitted in a standalone TRNG system.

3.3.2 Software Framework

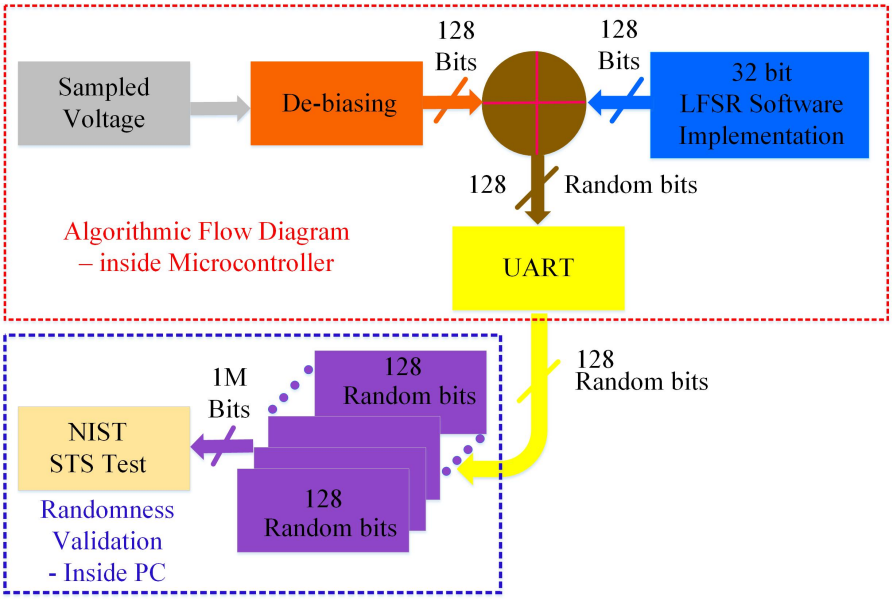

Figure 3.4: Software schematic of proposed TRNG (© 2020 IEEE).

The software framework (shown in Figure 3.4) for the proposed TRNG implements post-processing algorithms to extract 128-random bits. The goal of the software framework was to make it as simple as possible to get adapted in resource-constrained embedded computing nodes in IoT. It has two major chunk operations, categorized based on the place of execution. The first part is implemented inside the microcontroller and it is an obligatory portion. The second portion, implemented inside PC, is discretionary and used to determine the health of random bits. The second portion is not part of the final design and once the randomness is validated it is dropped off. The following major operations are performed in the software framework:

Sampling

The 12 bit ADC has 0.8 mv resolution, which is sufficient to detect typical variations of 200 mv in photoresistor voltage at a given light intensity. The sampled voltage of the same sensor is compared with the previously sampled voltage of the sensor to generate a bit. The bit is '0', if the sampled ADC voltage is the same or less, otherwise it is '1'.

Debiasing

The first bits generated from sensor voltages are usually biased and debiasing is required to produce the random bits. There exist several debiasing techniques, for example, cryptographic hash functions, deterministic extractor functions, resilient functions, and correcting functions[44][76]. In this research work, the von Neumann correcting function is chosen due to its lower computing and memory requirements. These properties are highly desirable for the proposed TRNG to get adapted for implementation in lighter IoT nodes. The von Neumann correcting function rejects any successive occurrence of bit "00" and bit "11". The bit sequence "01" and "10" is accepted as bit '0' and bit '1' respectively.

Ex-OR with LFSR output bits

This part is the key and core of the TRNG framework. When sensors response is changing slowly and sampled at high frequency, we observed that in the worst case they may produce raw bit strings of repeated "10" or "01" of some bit length. It would result in an uninterrupted sequence of identical bits (i.e. long runs) at the output of the von Neumann correcting function. The true random source is expected to have runs of 0s and 1s of different lengths with expected frequency. However, too many or too small lengths of runs and with high-frequency results in poor randomness. One possible solution to reduce long-biased bits is to sample the sensors at a low rate, however, it could result in a lower random bit generation rate.

In our proposed prototype, we do the Ex-OR operation (Ex-ORing with LFSR bits) of two 128 bit chunks: First from the output of the von Neumann debiasing function and other from software implemented 32-bit maximum length Linear feedback Shift Register (LFSR). We chose 32 bit LFSR because it has a large period of 4294367295 bits and can provide different 128-bit chunks at each Ex-Or operation. We will show in the next section that this method fixes the lower entropy at the dark light condition and removes the problem of long runs of 1s and 0s.

3.4 Experimental Setup and Results

The ideal TRNG should work independently from changes in the quantity being sampled. The proposed TRNG was subjected to varying light condi-

tions inside a light chamber, as shown in Figure 3.5. The NIST STS has 15 tests to validate randomness[110]. We collected 1 million bits (one sequence) at light intensity 0 W/m^2 (extreme dark) to 40 W/m^2 (normal sunlight). A test with a p-value ≥ 0.01 indicates that the sequence is random with 99 % confidence and the test is passed.

Figure 3.5: Experiment setup (© 2020 IEEE).

The efficacy of the additive scrambling (Ex-ORing with LFSR bits) approach can be checked in two ways, first by entropy measurement and second by passing NIST tests. Figure 3.6 uses Shanon's entropy equation to plot entropy for random bit sequence and validate the claim of improved entropy at dark light. The entropy after additive scrambling is ≈ 1, which indicates high uncertainty. Further, it is evident from the first two test results in Table 3.1 that additive scrambling helps to pass all 15 NIST STS test.

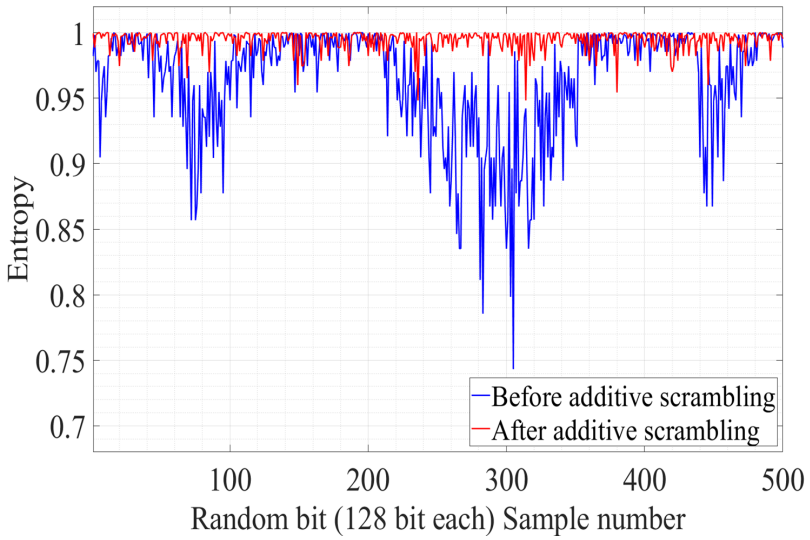

Figure 3.6: Effect of additive scrambling on Entropy at light intensity 0 W/m^2 (© 2020 IEEE).

3.4.1 NIST Statistical Test Suite results

Each NIST STS test checks a random bit sequence for a unique purpose, which is listed in NIST guideline[111]. Due to the abrasive nature of the random bit sequence, the criteria for each test is different. The non-overlapping template, random excursion, and random excursion variant test have 148, 8, and 18 sub-tests respectively. The p-value for the above tests is an average value of all sub-tests in Table 3.1. Further, to perform random excursion and random excursion variant tests, the random bit sequence should pass the frequency test and has several cycles greater than 500 [111]. The term not applicable (n/a) in Table 3.1 points out that the relevant test is skipped due to an insufficient number of cycles by the test suite.

The exhaustive test for randomness verification was performed to find anomalous behavior of the proposed TRNG. We collected 100 sequences to subject to NIST STS testing. The natural environment was simulated by randomly varying light conditions from extreme dark to full at a random interval. Further, we obstructed light falling on any randomly chosen sensors at a random time during operation. Table 3.1 lists the p-value for exhaustive tests and is practical proof that the prototype can tolerate the change in ambient light.

Table 3.1: NIST Statistical Test Suite results. Result is 'pass', if p-value > 0.01 (© 2020 IEEE).

Test name	p-value Ex-OR LFSR		p-value at different light intensity					Exhaustive Test		
	without	with	0 W/m^2	10 W/m^2	20 W/m^2	30 W/m^2	40 W/m^2	p-value	Proportion	Result
Frequency	***0.000000***	0.156099	0.227307	0.923738	0.083471	0.939268	0.548669	0.816537	0.9900	**Pass**
Block frequency	***0.000000***	0.927501	0.954847	0.739690	0.828306	0.241850	0.343236	0.851383	1.0000	**Pass**
Cumulative sums (forward)	***0.000000***	0.126651	0.279898	0.762967	0.058918	0.989132	0.535035	0.096578	0.9900	**Pass**
Cumulative sums (reverse)	***0.000000***	0.249778	0.248341	0.673262	0.075123	0.965337	0.489175	0.514124	0.9800	**Pass**
Runs	***0.000000***	0.866566	0.870771	0.105751	0.246265	0.446113	0.559371	0.455937	1.0000	**Pass**
Longest run	***0.000000***	0.864463	0.687594	0.873904	0.096038	0.435841	0.842273	0.289667	1.0000	**Pass**
Rank	***0.004280***	0.250500	0.669781	0.903934	0.608650	0.281791	0.964394	0.759756	0.9900	**Pass**
FFT	***0.000000***	0.453635	0.264045	0.556518	0.217423	0.812934	0.756450	0.978072	0.9800	**Pass**
Non-overlapping template (148)	***0.000000***	0.469966	0.488747	0.481182	0.501738	0.511771	0.551411	0.501522	0.9879	**Pass**
Overlapping template	***0.000000***	0.567448	0.898972	0.332220	0.266956	0.883922	0.557932	0.494392	0.9800	**Pass**
Universal	***0.000000***	0.762748	0.101559	0.273205	0.096837	0.883723	0.189590	0.383827	0.9900	**Pass**
Approximate entropy	***0.000000***	0.753883	0.630872	0.045073	0.016413	0.529153	0.720651	0.534146	1.0000	**Pass**
Random excursions (8)	***n/a***	*n/a*	0.720551	0.559315	*n/a*	0.507115	*n/a*	0.421557	0.9927	**Pass**
Random excursions variant (18)	***n/a***	*n/a*	0.482817	0.425737	*n/a*	0.537126	*n/a*	0.225245	0.9943	**Pass**
Serial-1	***0.000000***	0.888561	0.464811	0.041445	0.983962	0.448933	0.342303	0.637119	0.9800	**Pass**
Serial-2	***0.000000***	0.584569	0.214004	0.311381	0.882605	0.545856	0.189946	0.616305	1.0000	**Pass**
Linear complexity	0.381449	0.968967	0.956401	0.767418	0.835116	0.327585	0.011104	0.171867	1.0000	**Pass**

The additive scrambling and exhaustive test was performed at varying light intensity from extreme dark to normal sunlight.
The minimum pass rate for each statistical test with the exception of the random excursion and random excursion variant test is 96 for 100 binary sequences.
The minimum pass rate for the random excursion and random excursion variant test is 65 for 69 binary sequences.

3.4.2 Data rate results

The data rate for random bit generation was calculated using the tick count of in built SysTick Timer of the microcontroller. We calculated the delay of the random bit generation algorithm for 100k samples, each one of 128 random bit. The speculated random bit generation rate is plotted in figure 3.7 for all sample values. The average random bit generation rate for the proposed TRNG is 8 kbps, which is higher than the current maximum reported (250 bps) in[71] among sensor-based TRNG, to the best of our knowledge.

3.5 Summary

The proposed TRNG has a simple electronic hardware and software framework that is suitable for integration in existing photoresistor based IoT node. The Ex-OR operation of the row sensor signal and LFSR is a novel method that helps to achieve high entropy (≈1) and pass all mandatory NIST STS tests to examine randomness. Additionally, this method helps to achieve a faster random bit generation rate. The proposed photoresistor based TRNG works satisfactorily at light conditions varying from extreme dark to normal sunlight and can tolerate random changes in light intensity. To the best of our knowledge, the average random bit generation rate of 8 kbps of the proposed prototype is better in current sensor based TRNG research. The proposed

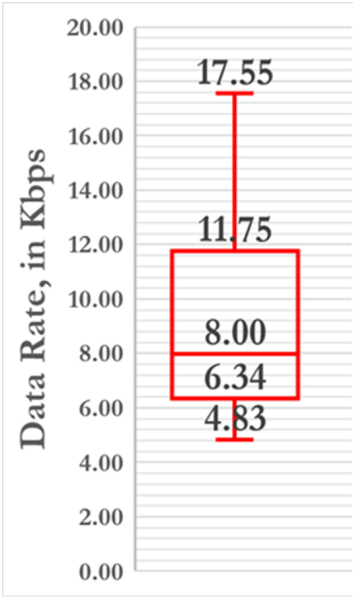

Figure 3.7: Random bit generation rate for proposed TRNG (© 2020 IEEE).

TRNG can be used in IoT cryptographic operations such as key generation in symmetric and asymmetric encryption, creation of Digital signature, and random vector in a stream cipher.

Chapter 4

Integrated TRNG-PUF Architecture based on PV Solar Cells for IoT

True Random Number Generator (TRNG) and Physically Unclonable Function (PUF) are inherently different architecture in a way they are designed. Unifying them as one architecture can be advantageous for computing power, memory and space limited smart computing devices.

The research work presented in this chapter was previously published in [52] as A. Degada and H. Thapliyal, "An integrated trng-puf architecture based on photovoltaic solar cells," IEEE Consumer Electronics Magazine, vol. 10, no. 4, pp. 99-105,

4.1 Introduction

The IoT integrates sensors, computing platforms, and networking among constituent blocks. The application space of IoT includes many intelligent consumer electronics appliances such as in aerospace, smart-home, vehicles, manufacturing plants, healthcare, real-time traffic monitoring, chemical process control, environmental monitoring, and smart-grid [128] [129], [130]. The inherently decentralized framework is a blend using networking technology and subsequently provides many vulnerable points to compromise security. Therefore, it is challenging to ensure confidentiality, integrity, authenticity, and availability across different physically integrated devices [27].

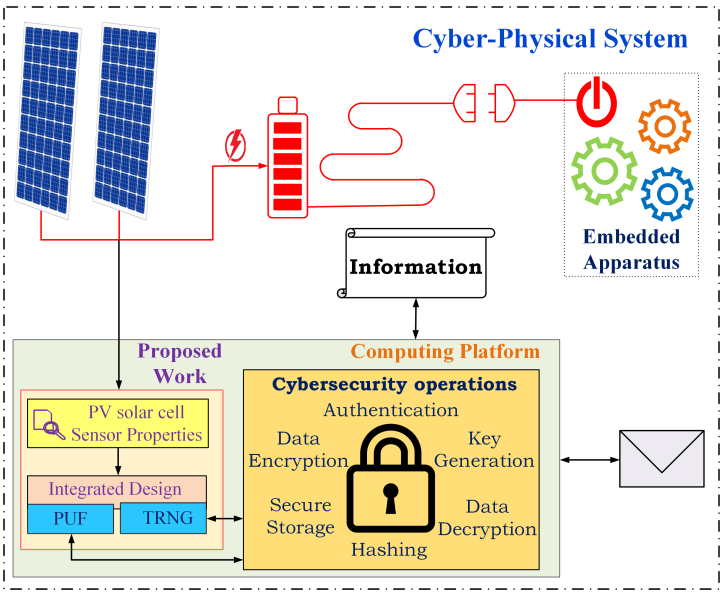

Figure 4.1: Building security primitives from solar cell sensors (© 2020 IEEE).

The use of renewable energy sources to fulfill energy requirements is a convenient way in the decentralized framework of IoT. The solar panels, as shown in Figure 4.1, are preferred to supply the energy need in many embedded apparatus in IoT. The Photovoltaic (PV) solar cell panels are preferred way to harvest solar energy in IoT and thereby, PV solar sensors find commonplace in many IoT applications[48]. Therefore, designing TRNG and PUF using sensors (in our case PV solar cell sensor) and microcontroller-based computing platform is a novel research direction.

The integration of TRNG and PUF as integrated architecture is a challenging task because of the fundamental difference of the PUF and TRNG design. There are existing works that have demonstrated the integrated TRNG-PUF architecture based on Field Programmable Gate Array (FPGA) [131] and CMOS [8], [132]. However, to the best of our knowledge, there is no existing work on integrated TRNG-PUF design based on Photovoltaic (PV) solar cells. Therefore, this article proposes integrated TRNG-PUF architecture devised around a common entropy source of Photovoltaic (PV) solar cells. Further, the proposed architecture does not require additional hardware and can be ported across the existing framework.

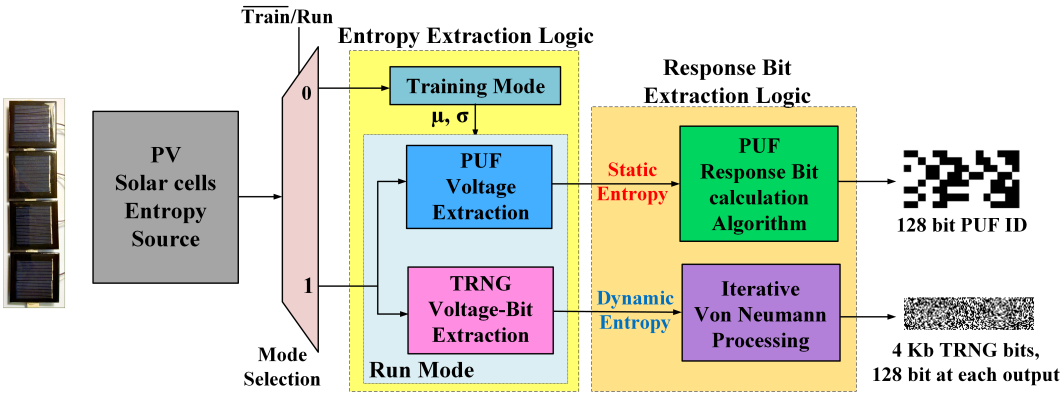

Figure 4.2: Schematic of integrated TRNG-PUF architecture (© 2020 IEEE).

4.2 Integrated TRNG-PUF Architecture

The proposed prototype shown in Figure 4.2 operates in two modes: (i) Training, and (ii) Run.

- The training mode learns the entropic nature of PV solar cells. The mean value (μ) and Standard Deviation (SD) (σ) of each solar cell voltage histogram is recorded. Additionally, the training mode sets an optimal sampling interval, a vital step to set optimum TRNG throughput. The detailed explanations are presented in the subsequent sections.

- The run mode segregates sensor response in either dynamic (large variation) response to produce TRNG output or static (stable) response to generate PUF output. The prototype has an option to enter in training mode before producing each TRNG/PUF response. The updated training information can reflect the change in response due to light intensity variations.

4.2.1 TRNG bits Generation

The TRNG transform randomness in entropic source to generate random bits. The proposed prototype produces initial binary streams by comparing the successive voltage samples produced outside one SD (σ) around mean (μ) in voltage histogram. However, the natural random source has a high

correlation between the successive samples, and post-processing becomes inevitable. There exist many techniques for post-processing, and among them, Von Neumann (VN) is particularly useful for limited computing power and small memory size. The proposed prototype implements the Iterative Von Neumann (IVN) approach to reduce wastage of initial binary streams ($\approx$ 76%)[133] in a single Von Neumann block.

4.2.2 PUF bits Generation

Over the years, many researchers have attempted to design the PUF using sensors. The electrical voltage of PV solar cells should have a predictable relationship with environmental conditions, e.g. ambient light for PV solar cells. Further, the response of many samples should settle to a static value. Additionally, the algorithm chosen should require less computing power and memory for IoT applications. One such algorithm is proposed in our earlier works [134] and the proposed prototypes in this research adapt the same method. The prototype produces a PUF response bit by calculating average voltage over one standard deviation (σ) around the mean (μ). This approach helps to reject outlier sample voltage response that typically arises naturally and thereby calculates a more stable voltage response.

4.2.3 Electrical Schematic of proposed prototype

Figure 4.3 is one of the possible ways to implement the proposed architecture and it can be explained in three steps. In step 1, the Analog-to-Digital Converter (ADC) samples eight PV solar cell sensors and converts voltage value into an equivalent digital reading. The next step implements training and run mode. In addition to that, CPU also implements an algorithm to produce 128-bit PUF response and IVN technique to produce 128-true random bits. In step 3, the TRNG and PUF response bits can be communicated further to perform cryptographic co-processor functions.

4.3 Entropy Extraction Logic

The PV solar cell is a p-n junction diode, and its output voltage depends on several variables. These variables include manufacturing process variations between sensors, the number of photons falling over the p-n junction, lifetime

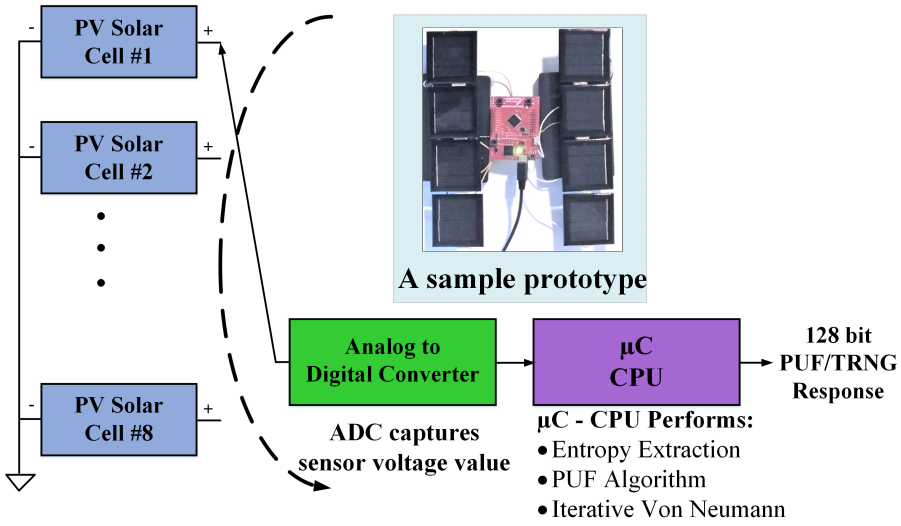

Figure 4.3: An example electrical schematic (© 2020 IEEE).

of electron-hole, doping of p and n-type material, area of the p-n junction and mobility of the charge. As these variables are random, we hypothesize that the photovoltaic solar cells could be a good entropic source.

A PV solar cell was connected to the ADC of the microcontroller. The output of the ADC is processed for analysis. The experiment setup was put under a light chamber that facilitates constant light source and isolation from the external light source. Figure 4.4 shows the histogram plot for the PV solar cell sensor for a total of 100,000 samples. The sensor follows the normal distribution. Important observations from Figure 4.4 are summarized as follow:

- The PV solar cell follows near-normal distribution for sampled voltages.
- The voltage samples within one SD (σ) around mean (μ) value can be utilized to calculate the average value, that would be relatively more stable. Later, it can be useful to calculate PUF response bits as per algorithm in [134].
- The successive voltage samples other than one SD (σ) around mean (μ) value would be useful to generate raw binary bits.

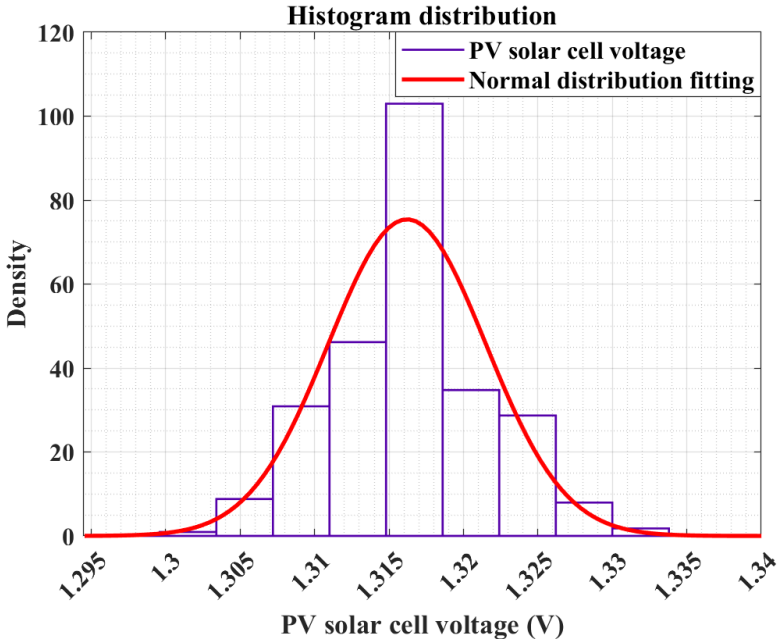

Figure 4.4: PV solar cell sensor voltage histogram (© 2020 IEEE).

4.4 Iterative Von Neumann (IVN) Processing for TRNG

A practical entropic source produces random bits 1 and 0 with unequal probability p and q respectively with some bias n. The number of unbiased bits is equal to npq and is far less than the achievable entropy bound. The bias makes the extraction of TRNG bits very difficult and depends upon sampling interval between two samples and environmental factors, such as external lighting, temperature, or humidity. The following equation originally described in [133] is used to calculate the bias:

$$n = \frac{|p - q|}{2} \times 100\% \tag{4.1}$$

The bias among initially generated raw bits arises due to a higher correlation between successive samples. High bias leads to rejection of raw bits, and therefore an optimum bias is desirable. The bias value 10% is a good balance between throughput and Shannon entropy per bit[133]. The Algo-

Algorithm 2 Input bit stream bias adjustment (© 2020 IEEE).

```
1: procedure BIAS-ADJUST(bits, S, δ)
2:     bits[ ] ← Array of initial bits
3:     S ← Set initial sampling Interval
4:     η ← Bias Value
5:     δ ← Set step value
6:     while η ≠ 10% do
7:         Generate 1000 sample bits in bits[ ]
8:         Calculate bias η
9:         if η >10% then
10:            S = S − δ
11:        else if η <10% then
12:            S = S + δ
```

rithm 1 is part of the training mode. It sets the bias value equals to 10% by adjusting sample interval (time difference between two successive samples). The process begins with generating 1000 raw bits and calculating the bias. Then, bias value is checked if it is >10% then subtract step value δ else add step value δ in initial step interval.

After setting the bias value 10%, the prototype switches to run mode to generate true random bits[133]. The initial input raw bit sequence is fed to the IVN tree structure realized using 7 Von Neumann blocks illustrated in Figure 4.6. The Von Neumann debiasing, shown in Figure 5a, is a suitable technique for low-computing-power and low-memory devices due to its simpler operation. It rejects successive occurrence of bit sequence "11" or "00" in output Von Neumann sequence and accepts bit sequence "01" and "10" as a bit '0' and '1' respectively. However, a single Von Neumann can extract throughput only up to 24%, a substantial loss of the bits.

Therefore, it becomes important to process entropy present in discarded bits. As implied in the name IVN, we process the Ex-OR and residual sequence to extract entropy present in them. We made some design choices to accommodate prototype for computing resource constraint platforms. First, we limit the structure up to 7 VN blocks as additional VN blocks would not result in much throughput improvement. Second, the residual sequence is processed only at two blocks, where the bias in residual sequences is relatively higher. The final TRNG outcome is produced by concatenating the output from all Von Neumann sequences and has $\approx 33.69\%$ better through-

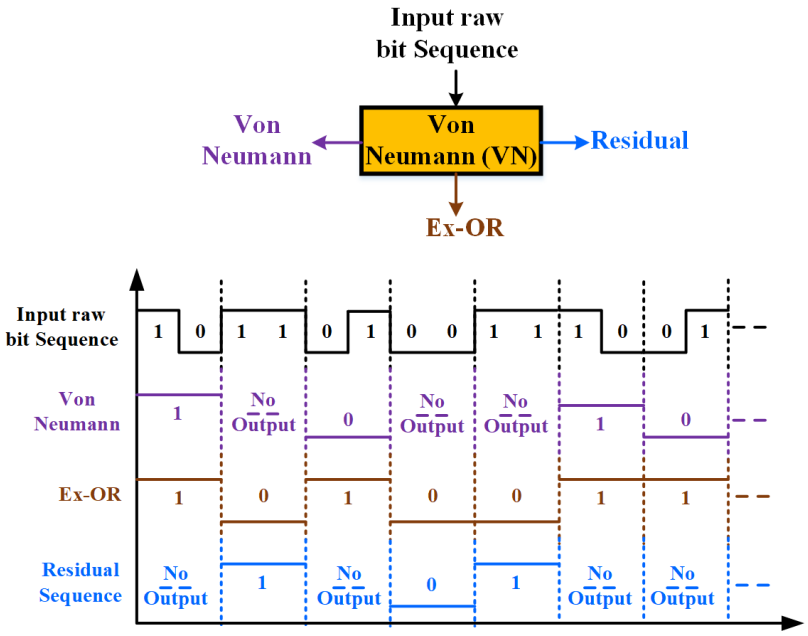

Figure 4.5: Von Neumann block and corresponding waveforms of output sequences (© 2020 IEEE).

put than a single Von Neumann.

4.5 Performance Testing

The TRNG and PUF are inherently orthogonal in operation, therefore, the metrics to measure the performance characteristic are quite different. Further, the change in light intensity can alter the electrical parameters of the photovoltaic solar cell. Thus, the change in light intensity is a useful environmental condition to vary to test the performance. An ideal design should work well at every light intensity. The experimental set up was placed inside a light chamber that facilitates the change in light condition from light intensity 0 W/m^2 (extreme dark) to 90 W/m^2 (very bright sunlight).

4.5.1 PUF Performance Testing

The reliability and uniformity metrics are used to measure the performance of the proposed PUF prototype. The PV solar sensors and microcontroller

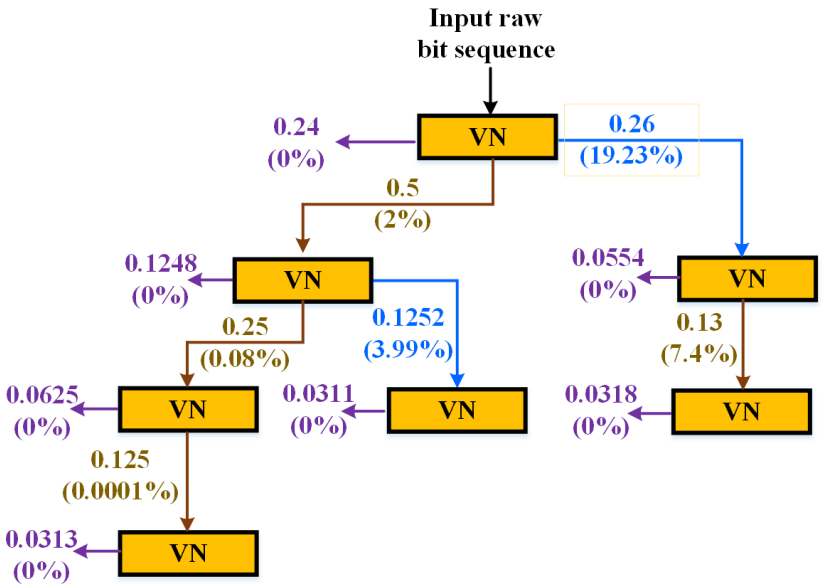

Figure 4.6: IVN tree structure using Von Neumann blocks. The value at output sequence is throughput with respect to reference value 1 (input bit sequence) and corresponding value in bracket indicates bias in percentage (© 2020 IEEE).

set up were put inside the light chamber and PUF output bits were recorded in PC.

Reliability

The reliability metric is the measure of the deviation of the PUF bit response with the reference response. It uses the hamming distance and is a measure of the reproducibility of PUF response with reference response. The following equation was first used to calculate reliability, R of n-bit PUF response

$$\mathrm{R} = 100\% - \frac{1}{M}\sum_{m=1}^{M}\frac{HD\left(R_{ref}, R_{m,t}\right)}{n} \times 100\% \tag{4.2}$$

The light intensity at 50 $\mathrm{W/m^2}$ (corresponding to normal room light intensity) was considered as the reference point. The Hamming Distance (HD) measures that how many bits are different between reference response, $\mathrm{R_{ref}}$, and response generated at different light conditions $\mathrm{R_{m,t}}$. Figure 4.7

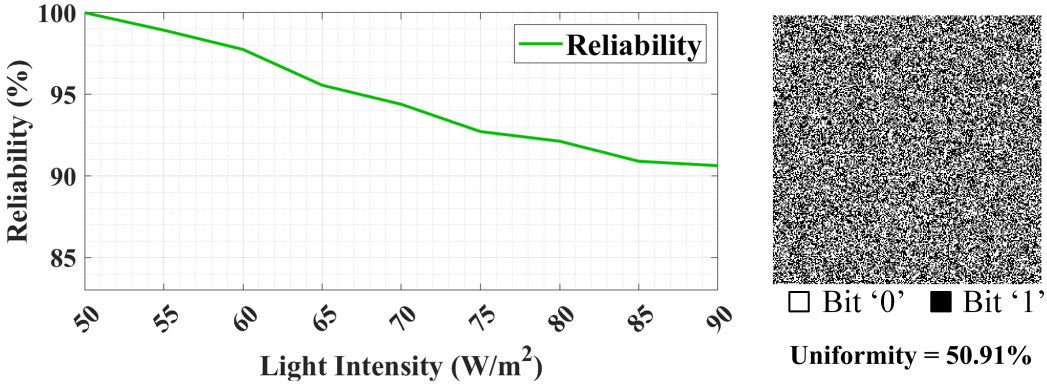

Figure 4.7: Reliability and Uniformity as a measure of PUF performance metric (© 2020 IEEE).

shows the measured reliability at a different light intensity. The proposed design has worst-case reliability of 92.13% at light intensity 90 W/m^2 and average reliability of 92.13% for light intensity variation from 50 W/m^2 to at 90 W/m^2.

Uniformity

The uniformity measures the proportion of 0 and 1 in PUF response. The ideal PUF response should have 50% uniformity, i.e. in 128-bit PUF response, the number of 0-bits and 1-bits should be 64.

The light intensity 50 W/m^2 was considered as reference and 12 different readings were taken at an interval of 1 hour. The worst-case uniformity is 47.66% and the best case uniformity is 50%. The average uniformity was measured at 50.91%, i.e. very close to the ideal value.

4.5.2 TRNG Performance Testing

The ideal TRNG should work independently of ambient light conditions. The quality of a random number is measured by different tests, e.g. NIST STS, DieHard, AIS, and TestU01. Among, them NIST STS is most widely used by researchers [44], [8], thus we preferred it in our work. The NIST STS is a collection of 15 tests that a true random sequence should satisfy.

The different tests in NIST STS check the number of occurrences of bits 1 and 0, find the run length, i.e. the number of consecutive occurrences of bit

1 or zero, checking linear dependence among the sub-string of, periodicity of occurrence in given length and ability to compress the sequence. Each test is measured by calculating "p-value", which indicates the confidence of randomness. A test with a p-value of $\geqslant 0.01$ indicates the test is passed and with 99% confidence. The nature of each random test is different and hence, the criteria for each test are also different. We collected a total of 100 random number sequences, where each sequence consists of 1 million random bits with light varied at the random interval to simulate the real-world scenario. Further, we exposed some sensors to light and some sensors were blocked during the data collection procedure. The minimum pass rate for each test other than random excursion and random excursion variant is 96 out of 100. The criteria to pass the random excursion and random excursion variant test are 65 out of 69 random bit sequences.

Table 4.1: NIST STS for TRNG evaluation. Result is 'pass', if p-value $>$ 0.01 (© 2020 IEEE).

Test name	Exhaustive Test		
	p-value	Proportion	Result
Frequency	0.845629	0.9900	**Pass**
Block frequency	0.451279	1.0000	**Pass**
Cumulative sums (forward)	0.152695	0.9900	**Pass**
Cumulative sums (reverse)	0.847926	0.9900	**Pass**
Runs	0.562478	1.0000	**Pass**
Longest run	0.384567	0.9900	**Pass**
Rank	0.747956	1.0000	**Pass**
FFT	0.859674	1.0000	**Pass**
Non-overlapping template (148)	0.501324	0.9937	**Pass**
Overlapping template	0.569541	0.9800	**Pass**
Universal	0.659841	0.9900	**Pass**
Approximate entropy	0.356947	1.0000	**Pass**
Random excursions (8)	0.846259	0.9927	**Pass**
Random excursions variant (18)	0.395846	0.9943	**Pass**
Serial-1	0.756185	0.9900	**Pass**
Serial-2	0.869416	1.0000	**Pass**
Linear complexity	0.231567	1.0000	**Pass**

Table 4.1 lists the results of each NIST test in terms of the p-value, the proportion of the test passed and the result of the test as either pass/fail.

The number in the bracket next to each test denotes, number of sub-tests. The proportion simply indicates how many random sequences passed for the test, with 1 indicating all 100 or 69 random bit sequences have cleared the test. The proposed prototype passes all tests with a very high p-value, with the lowest 0.231567 and the highest 0.845629. The average p-value for all the tests is 0.45.

4.6 Summary

The research work in this article proposes an integrated design of TRNG and PUF using PV solar cells and the microcontroller. We have shown that the voltage response of PV solar cells can be engineered in static (stable) and dynamic (large variation) response. The segregation is based on dividing the PV solar cell histogram within or outside one SD (σ) around the mean voltage value (μ). The proposed prototype uses Iterative Von Neumann (IVN) structure which has $\approx$ 33.69% better throughput to generate true random bits. The proposed prototype achieves an average 92.13% reliability and 50.91% uniformity in PUF response. The integrated TRNG-PUF architecture can be beneficial in space-limited IoT.

Chapter 5

2-Phase Symmetric Pass Gate Adiabatic Logic (2-SPGAL) to design secure and energy-efficient cryptographic circuits

In recent years, researchers have shown that it is relatively simple to extract the secret encryption key using Side-Channel Attack. On the other hand, the healthcare sector is a lucrative target for the attacker as the data present in the system has huge value, and the networking of many smart devices provides multiple entry doors. In this research, we use the energy-recycling principle that allows building Correlation Power Analysis (a type of Side-Channel Attack) with a significant saving of the energy consumption.

The research work presented in this chapter was previously presented in [10] as 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, and currently under review in [53] as A. Degada and H. Thapliyal, "2-phase adiabatic logic for low-energy and cpa-resistant implantable medical devices," IEEE Transactions on Consumer Electronics, pp. 1-10, 2021.

5.1 Motivation

According to the World Health Organization report, 1.9 billion adults were overweight, and out of which 35% were obese in 2017. Further, 340 million children and adolescents were obese or overweight in 2020. Higher body weight can lead to chronic diseases, such as cardiovascular diseases, hypertension, diabetes, degenerative to joints, musculoskeletal system disorders, and several cancers, e.g., liver, colon, ovarian, gallbladder, kidney, breast, and prostate [135]. The US Centers for Disease Control (CDC) classify obesity at epidemic proportions. The CDC reports say 6 in 10 adults in the US have a chronic disease and 4 in 10 adults suffers more than one chronic disease [136]. On the other end, the advancement in semiconductor technology has empowered the inclusion of medical devices in many chronic disease diagnostic, therapeutic processes, and patient monitoring. They are pervasive in medical labs, offices of physicians, and even implanted inside a patient's body, e.g. pacemaker, Implantable Cardiac Defibrillators (ICDs), and neurostimulators. Table 5.1 lists some of the medical devices and their frequency range of the operation.

Table 5.1: Frequency range in medical applications.

Reference	**Medical Application**	**Frequency range of operation**
[**137**]	Low frequency inductive implants (pacemakers, ICD etc.)	Less than 200 kHz
[**138**] [**139**]	Implant communication	9 - 315kHz
[**140**]	Bioelectrical impedance meter	50 kHz, 250 kHz
[**141**]	Electrical Impedance Myography (EIM)	50 kHz
[**142**] [**143**] [**144**]	Electrical Impedance Tomography (EIT)	50 kHz to 250 kHz
[**145**]	CMOS wearable non-invasive impedance meter	100 Hz to 1 MHz
[**146**]	Hearing Aid	32 khz to 8.00 Mhz
[**147**]	Magnetic Particle Imaging (MPI) systems	1 kHz to 100 kHz
[**148**] [**149**]	Low data-rate Body Couple communication (BCC)	10 kHz to 10 MHz
[**150**]	Home Health Hub	200 kHz to 1.0 MHz

Modern medical devices often aggregate physiological data, store the personal information of the patient and communicate to the cloud. Some of these

devices, e.g. medical implants are battery-powered and their operational life is limited up to 10 years [151] [152]. Over the years, many researchers have raised concerns about compromising sensitive personal and physiological information. The compromised device can perform unauthorized command execution and data transmission [40], create electrical shocks [42] [43] and deplete battery [41]. It can compromise the secrecy and privacy of the patient information, however, in some cases it could be life-threatening. It becomes of utmost importance to protect user-information by including cryptographic coprocessors in device design. Security often comes with the cost of increment in the power consumption [153] [33] [154] [155]. Therefore, designing energy-efficient and secure cryptographic coprocessor circuits in medical devices is an interesting research direction.

Lightweight Cryptographic (LWC) cipher is one of the preferred solution to provide encryption at low-energy budgets [156], [157], [158]. However, in recent years, the LWC ciphers have been found vulnerable against Side-Channel Analysis (SCA) attacks, e.g. heat emission, electromagnetic radiation, power analysis [101], [91], and timing attacks [99]. The work in [148] [159] lists several possible SCA over medical devices. Among different possible SCA, the Correlation Power Analysis (CPA) attack is easy to implement and found more lethal to reveal the encryption key.

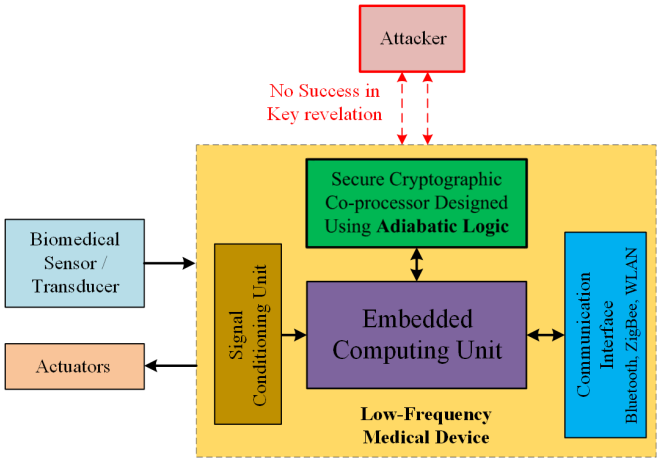

Figure 5.1: Adiabatic Logic as preferred choice to design energy-efficient and secure cryptographic coprocessor.

In this article, we use adiabatic logic to design energy-efficient and secure lightweight cryptographic coprocessor in medical devices (Figure 5.1).

The adiabatic logic circuits recover the energy stored inside the load capacitor (rather than dissipating as heat), thus, results in significantly low-power consumption. Further, the power traces of the adiabatic logic circuits are uniform in shape, unlike the conventional CMOS logic circuits. The uniform power traces is a very important property to disguise the processed information. The above property helps to combat the CPA.

The adiabatic logic is a low-power circuit design technique that recovers the charge stored inside the load capacitors, and thus reduces the significant energy consumption compared to the conventional CMOS logic. The physiological signals of human bodies are typically low-frequency values [160], [161], [138]. Conventional ultra-low-power medical devices and operate over tens to a few hundred kilohertz of the frequency range. As adiabatic logic operates energy efficiently at low frequency, therefore in this work, we proposed to design low-energy and secure cryptographic co-processors based on adiabatic logic. Further, the adiabatic logic circuits have uniform power traces, thereby "hides" the information leakages. Therefore, the proposed LWC circuit based on adiabatic logic will be resilient against the CPA attacks. To validate our hypothesis, we present a novel 2-phase Symmetric Pass Gate Adiabatic Logic (2-SPGAL) and use it to design a low-energy and CPA resistant design of LWC PRESENT. The energy and CPA resilient capability of the adiabatic logic circuit largely depends upon the design of the power clock generator (PCG) [162], [163], [164], [165]. The PCG consumes a large fraction of the energy consumption, and its poor design can also affect security resilience. In this work, we evaluate the energy and security metrics of the proposed 2-SPGAL with two different synchronous resonant sinusoidal PCGs: 2N2P-PCG and 2N-PCG (Refer Section 2.5).

5.1.1 Key Contributions from this work

The key contributions of this work are as follows:

- The chapter presents 2-SPGAL, a novel 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL). The proposed 2-SPGAL can be a design choice for low-energy and CPA-resistant IMDs.

- The energy and security of the adiabatic logic largely depend upon the PCG integrated into the design. Therefore, we evaluated the energy

efficiency and CPA-resistance of the proposed 2-SPGAL with two different types of synchronous resonant Power Clock Generators (PCGs). Two types of PCGs are 2N2P-PCG and 2N-PCGs.

- The logic gates, AND/NAND and XOR/XNOR gates of 2-SPGAL are evaluated in terms of energy and security metrics with 2N2P-PCG and 2N-PCG integrated into the design.

- The one round of PRESENT-80 designed using proposed 2-SPGAL with 2N-PCG integrated into the design, shows an average of 47.50% energy saving compared to its CMOS counterpart design for the frequency range of 50 kHz to 250 kHz. The same design implemented with 2N2P-PCG integrated into the design shows an average of 51.18% energy saving compared to its CMOS counterpart over the frequency range of 50 kHz to 250 kHz.

- The one round of PRESENT-80 designed using 2-SPGAL with 2N2P-PCG integrated into design shows an average of 16.62% energy-saving compared to existing 2-phase adiabatic logic 2-EE-SPFAL [9]. Similarly, 2N-PCG integrated into the design shows an average energy saving of approximately 29% compared to 2-EE-SPFAL [9].

- The output of the PRESENT-80 S-box is considered as the attack point in literature. Its CPA resilience capability is measured in Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) metrics. The 2-SPGAL based S-box with 2N-PCG integrated shows an average improvement of 97.60% security performance improvement compared to CMOS counterpart over the frequency range of 50 kHz to 250 kHz. . Similarly, the 2-SPGAL based S-box with 2N2P-PCG integrated into design shows an average of 96.61% security performance improvement. Further, 2-SPGAL based S-box design has an average of 11.56% better security performance compared to its 2-EE-SPFAL [9] counterpart.

- We demonstrate that the PRESENT-80 using novel 2-SPGAL can successfully defend the encryption key against the CPA attack for both 2N2P-PCG and 2N-PCG integrated with the design. However, the encryption key is revealed in the same counterpart design using CMOS.

5.2 Proposed 2-Phase Adiabatic Logic Design

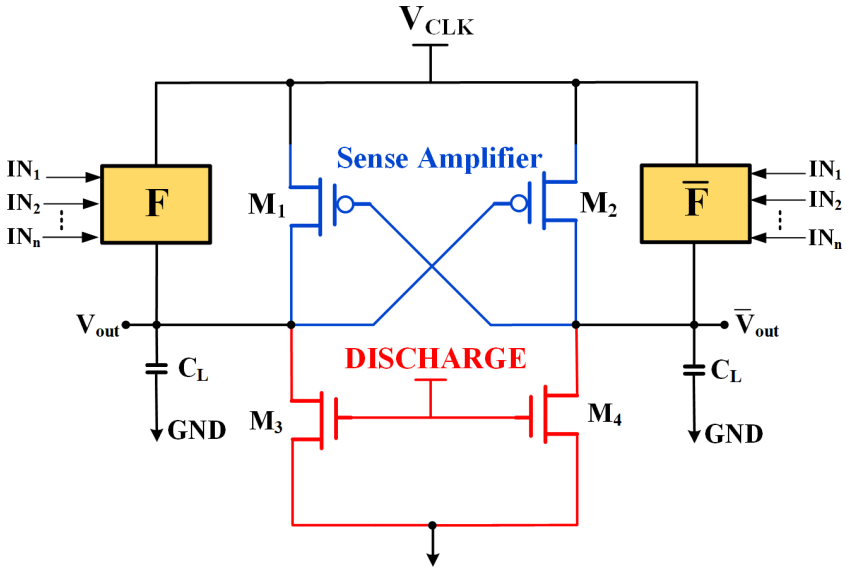

Figure 5.2: General SPGAL logic gate structure[6] (© 2021 IEEE).

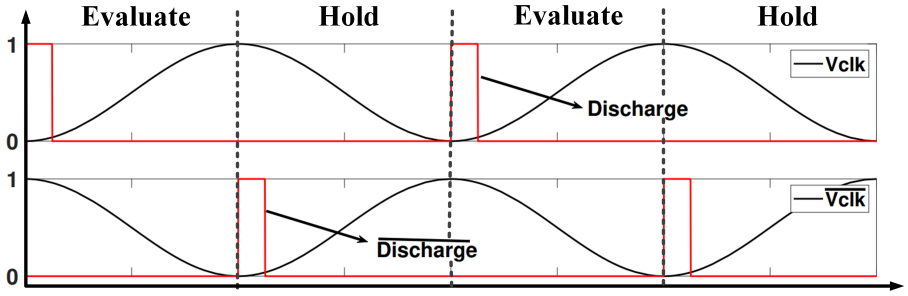

Figure 5.3: Sinusoidal clocking idea [9], [10] (© 2021 IEEE).

The Symmetric Pass Gate Adiabatic Logic (SPGAL) logic gate structure (Figure 5.2) consists of three blocks: a sense amplifier, a discharge circuitry, and logic evaluation blocks. The PMOS transistors M1, and M2 construct the sense amplifier/latch. The discharge signal turns the nmos transistor M3, and M4 to ON, and provides a discharge patch for residue charge stored in the load capacitor. The evaluation block transistors produce correct logic gate

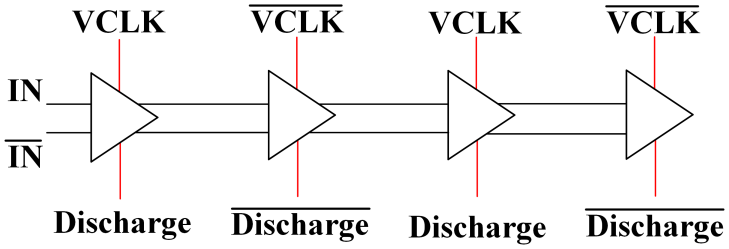

Figure 5.4: Four cascaded adiabatic buffers implemented in cascade using 2-phase clocking scheme [9], [10] (© 2021 IEEE).

output based on input logic signals. The SPGAL was originally proposed on a 4-Phase trapezoidal clocking scheme [6].

In this work, we hypothesize that the slow varying sinusoidal signal (Figure 5.3) can be a potential replacement for the trapezoidal clock. To check our hypothesis, the discharge signal is adjusted to the negative peak of the sinusoidal signal. The rising part of the sinusoidal signal is referred to as evaluate and the falling part is referred to as the recovery phase of the adiabatic operations. The two discharge signals are synchronous to the negative pick of the respective phase. The above 2-phase sinusoidal clocking implementation of SPGAL is referred to as 2-SPGAL. The adiabatic logic circuits operate in pipelined fashions. It was found (Figure 5.4) that the 2-phase sinusoidal clocking allows using two out-of-phase power clocks and discharge signals to operate a 4-cascaded 2-SPGAL buffer logic gate.

5.3 Energy and security evaluation of 2-SPGAL logic gates

The next step is to check the energy and security evaluation of 2-SPGAL gates at different frequencies with PCG integrated into the design. For an ideal secure circuit, the variation in energy consumption should be zero for all possible input variations. In a practical scenario, the lower variation in energy consumption comes from a smaller variation in current traces. Further, the CPA estimates the correlation between the leakage power and mathematical hypothetical power models. Hence, the success of CPA depends upon the linear dependency between the hypothetical power traces and collected power traces. The above linear dependency can be disguised if we have uniform

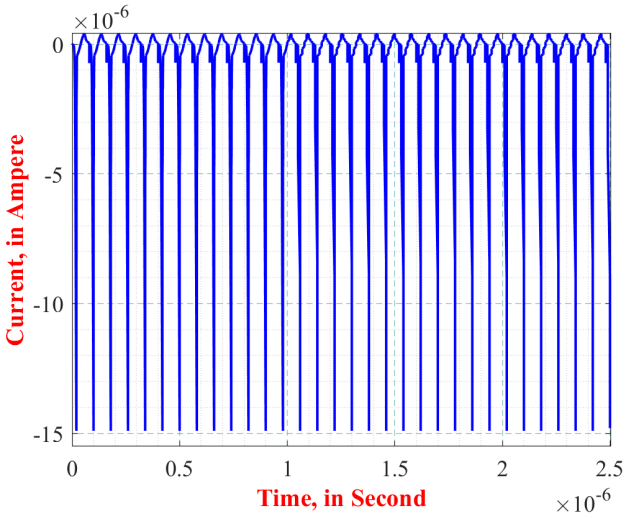

Figure 5.5: Uniform current in 2-SPGAL Ex-OR logic gate (© 2021 IEEE).

current traces. Figure 5.5 shows the current traces for XOR gates as an example. It can be observed that current traces 2-SPGAL based logic gates are uniform.

We performed the SPICE simulation to collect the energy consumption value for all possible input bit variations. For example, an n-bit circuit will have a total 2^{2n} possible cyclic variations. The NED and NSD metrics at different frequencies can give an idea about the security resilience of the 2-SPGAL gates against CPA attack. The smaller the NED and NSD values imply the more robustness against the CPA attack. They are calculated based on energy consumption in circuit for different input bit combinations. On the other hand, the energy and security evaluation of the adiabatic logic circuit largely depends upon the types of PCG integrated. Thereby, the energy and security metric of the logic gates should be compared with PCG integrated into the design.

Table 6.1 lists the simulation results for the proposed 2-SPGAL and the existing 2-EE-SPFAL [9] AND/NAND logic gate with 2N2P-PCG and 2N-PCG integrated into the design. Among the four different designed listed in Table 6.1, 2-SPGAL AND/NAND logic gate with 2N-PCG integrated into the design has superior performance. It has an average NED and NSD value of 1.669 and 0.518 respectively over the frequency range of 50 kHz to 250 kHz. The 2-SPGAL AND/NAND logic gate with 2N2P-PCG integrated into the

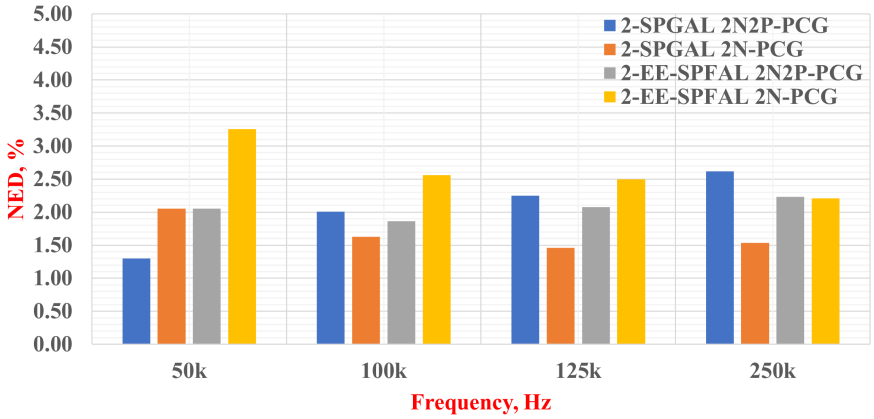

Figure 5.6: NED value comparison for AND logic gate.

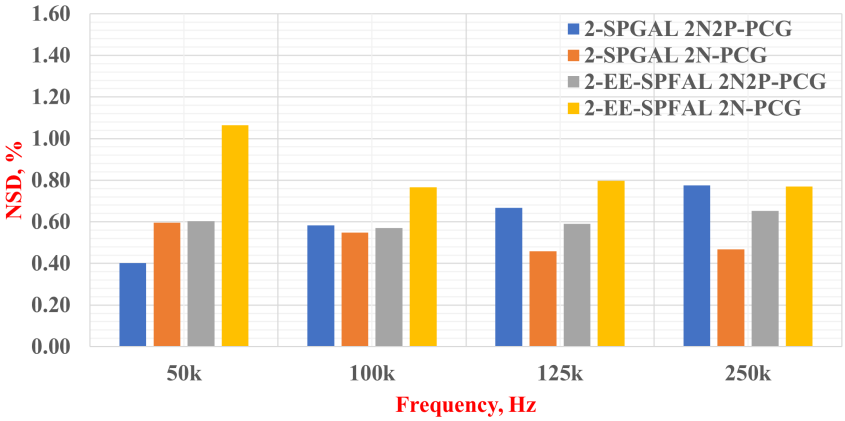

Figure 5.7: NSD value comparison for AND logic gate.

design, has an average NED and NSD metric value of 2.043 and 0.607. The average NED and NSD values for 2-EE-SPFAL [9] AND/NAND logic gate with 2N2P-PCG integrated into the design are 2.055 and 0.604 respectively, over the frequency range of 50 kHz to 250 kHz. The 2-SPGAL AND/NAND logic gate has identical CPA resilience capability with 2N2P-PCG integrated into the design compared to the 2-EE-SPFAL [9] counterpart. Further, the 2-SPGAL AND logic gate shows superior CPA resilience capability for 2N-PCG integrated into the design compared to 2-EE-SPFAL [9] AND/NAND logic gate counterpart.

Table 5.2: Energy-efficiency and security evaluation of the 2-phase AND logic gate with 2N-PCG and 2N2P-PCG.

Proposed 2-SPGAL AND Logic Gate								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{\min}(fJ)$	9.18	11.25	11.15	9.00	11.11	9.00	11.16	8.97
$E_{\max}(fJ)$	9.30	11.49	11.38	9.15	11.37	9.13	11.46	9.11
$E_{\text{avg}}(fJ)$	9.24	11.40	11.29	9.09	11.28	9.08	11.35	9.05
NED (%)	1.300	2.050	2.008	1.629	2.246	1.461	2.616	1.534
NSD (%)	0.402	0.596	0.583	0.548	0.667	0.459	0.776	0.467
2-EE-SPFAL AND Logic Gate [9]								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{\min}(fJ)$	11.86	7.40	11.75	5.18	11.70	5.40	11.76	6.28
$E_{\max}(fJ)$	12.10	7.65	11.98	5.32	11.94	5.54	12.03	6.43
$E_{\text{avg}}(fJ)$	12.02	7.50	11.89	5.26	11.86	5.48	11.94	6.37
NED (%)	2.052	3.258	1.862	2.558	2.073	2.497	2.231	2.211
NSD (%)	0.603	1.064	0.571	0.766	0.589	0.798	0.652	0.769

Similar to AND/NAND logic gate, we performed the simulation to collect energy numbers for the proposed 2-SPGAL XOR logic gate and 2-EE-SPFAL [9] XOR/XNOR logic gate with 2N2P-PCG, and 2N-PCG integrated into the design. Table 5.3 shows energy and security metrics comparison for proposed 2-SPGAL XOR/XNOR gate with 2-EE-SPFAL XOR/XNOR logic gate [9]. The 2-SPGAL XOR/XNOR logic gate has an average NED and NSD values almost equal to zero like its 2-EE-SPFAL [9] counterpart with

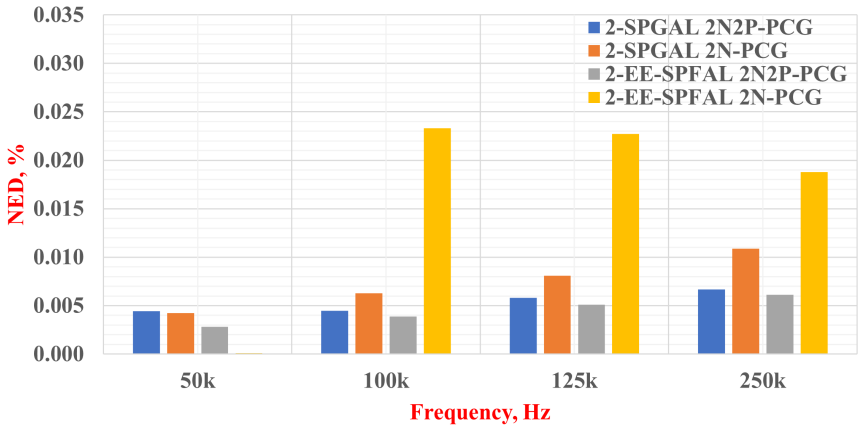

Figure 5.8: NED value comparison for XOR logic gate.

PCGs integrated into the design. This property is accounted for the balance of inputs on logic evaluation blocks. This results in a more symmetrically built load capacitance value. It results in equal switching activities of the XOR gate, thereby, more uniform power traces, therefore, almost ideal NED and NSD metric values.

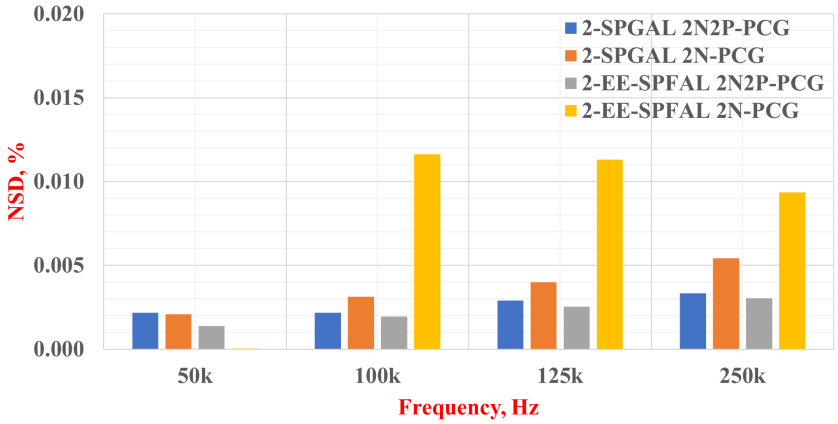

Figure 5.9: NSD value comparison for XOR logic gate.

Table 5.3: Energy-efficiency and security evaluation of 2-phase XOR logic gate with 2N-PCG and 2N2P-PCG.

2-SPGAL XOR Logic Gate								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{\min}(fJ)$	11.10	9.04	11.02	8.87	10.99	8.89	11.06	8.87
$E_{\max}(fJ)$	11.11	9.04	11.02	8.87	10.99	8.89	11.06	8.87
$E_{\text{avg}}(fJ)$	11.10	9.04	11.02	8.87	10.99	8.89	11.06	8.87
NED (%)	0.0044	0.0042	0.004	0.006	0.006	0.008	0.007	0.011
NSD (%)	0.0022	0.0021	0.002	0.0036	0.003	0.004	0.004	0.005
2-EE-SPFAL XOR Logic Gate [9]								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{\min}(fJ)$	11.71	7.62	11.58	5.19	11.56	5.36	11.63	6.19
$E_{\max}(fJ)$	11.71	7.62	11.58	5.19	11.57	5.37	11.63	6.19
$E_{\text{avg}}(fJ)$	11.71	7.62	11.58	5.19	11.56	5.36	11.63	6.19
NED (%)	0.0028	0.0001	0.004	0.023	0.005	0.023	0.006	0.019
NSD (%)	0.0014	0.0000	0.002	0.0012	0.003	0.011	0.003	0.009

5.4 Case study - PRESENT-80 one round of encryption design using 2-SPGAL

In this section, we illustrate the design of the PRESENT, a lightweight cryptographic cipher. The PRESENT is a simple, secure, and energy-efficient block cipher. The PRESENT block cipher is particularly suitable to the application which does not require large data to be encrypted, e.g. IMDs, RFID, IoT. The proposed 2-SPGAL can be a potential logic design option to design energy-efficient and secure IMDs.

5.4.1 PRESENT-80 implementation using proposed 2-SPGAL

The cryptographic circuits of the IMD should be low-energy as they operate in a limited battery budget. The PRESENT was originally proposed in [5] and recently received higher attention from the researchers due to its ability to meet low-energy encryption. Further, the counter mode operation of PRESENT enables its usage in challenge-response authentication protocols [166]. The PRESENT-80 comes up with two variants depending upon the size of the key, 80-bit, and 120-bit. The PRESENT-80 is 32-round of encryption, and out of which 31 rounds are identical. Therefore, we implemented one round of PRESENT-80 encryption using the proposed 2-SPGAL.

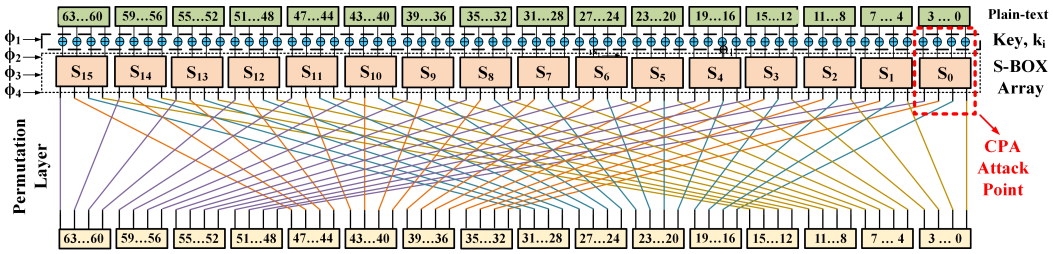

Figure 5.10: one round of PRESENT-80 implementation using 2-phase adiabatic logic (© 2021 IEEE).

Figure 6.8 shows the schematic of the case-study design of PRESENT-80 one round of encryption. The PRESENT-80 design has three fundamental operations. During addRoundKey operation the XOR operation of the plaintext is done with the key. The Substitution-box (S-box) does the non-linear

transformation in 4-bit chunks, with a total of 16 in parallel. The third operation is the permutation of the S-box output to add further randomization [5].

Table 5.4: Number of Transistor Required to implement PRESENT-80 one round [10] (© 2021 IEEE).

Adiabatic Logic	**2-EE-SPFAL [9]**	**Proposed 2-SPGAL**
Number of Transistor	9344	7776
2-SPGAL saves 16.78% transistor to its counterpart 2-EE-SPFAL [9]		

Table 5.4 lists the total number of transistors required to implement using proposed 2-SPGAL and 2-EE-SPFAL [9]. The SPGAL has two fewer transistors in its sense-amplifier structure of the gate. The 2-SPGAL based design requires 7776 transistors, while its counterpart designed using 2-EE-SPFAL needs 9344 transistors. This results in 16.78% fewer transistors in 2-SPGAL design compared to 2-EE-SPFAL [9]. The less number of transistors and simpler power clock routing can result meet the smaller layout and are the requirement for consumer IoT devices.

5.4.2 Energy-Efficiency comparison

$$E = \int_0^T V_P I_P dt \tag{5.1}$$

The energy consumption is the integration of the voltage and current product over the time period of the input signal. The V_{p} is voltage and I_{p} is the current from PCG or power supply [167]. We show the comparison of the average energy consumption for the one round of PRESENT-80 at 45nm technology with 10 fF load using (i) Proposed 2-SPGAL with 2N-PCG, and (ii) Proposed 2-SPGAL with 2N2P-PCG, (iii) 2-EE-SPFAL [9] with 2N-PCG, (iv) 2-EE-SPFAL [9] with 2N2P-PCG and (iv) conventional CMOS design. The cryptographic circuits are presented for low-frequency IMD devices, and therefore the frequency range of 50 kHz to 250 kHz is considered in this work.

The energy consumption is measured in terms of energy per cycle, i.e. average energy consumption value over all possible combinations of inputs [9]. Lower the energy per cycle value means better energy performance, and thus can be useful to design energy-saving IMDs. The energy per cycle

Table 5.5: Energy consumption (in pJ/cycle) in case study of one round of PRESENT-80 encryption.

Logic used to design case study	**PCG integrated in design**	**50 kHz**	**100 kHz**	**125 kHz**	**250 kHz**	**Average**
CMOS	–	2.376	1.569	1.409	1.092	**1.611**
2-EE-SPFAL [9]	2N-PCG	1.250	1.257	1.066	0.913	**1.121**
	2N2P-PCG	0.848	0.895	0.870	0.878	**0.872**
Proposed 2-SPGAL	2N-PCG	0.795	0.795	0.787	0.764	**0.785**
	2N2P-PCG	0.725	0.728	0728	0.728	**0.727**

Table 5.6: Energy saving (in %) comparison in proposed 2-SPGAL based one round of PRESENT-80 encryption.

PCG integrated in 2-SPGAL design	**Baseline Logic to compare case study implementation**	**50 kHz**	**100 kHz**	**125 kHz**	**250 kHz**	**Average**
2N-PCG	2-EE-SPFAL [9]	36.40	36.76	26.13	16.32	**28.90**
	CMOS	66.54	49.32	44.10	30.05	**47.50**
2N2P-PCG	2-EE-SPFAL [9]	14.47	18.66	16.31	17.02	**16.62**
	CMOS	69.49	53.39	48.31	33.31	**51.18**

for one round of PRESENT-80 designed using 2-SPGAL, 2-EE-SPFAL [9], and CMOS is shown in Table 5.5. The proposed 2-SPGAL logic base one round of PRESENT-80 shows overall superior performance compared to their CMOS and 2-EE-SPFAL counterparts for every frequency in the range of 50 kHz to 250 kHz. The average energy consumption (i.e. average energy for the frequency range 50 kHz to 250 kHz) for 2-SPGAL 0.727 pJ/Cycle and 0.785 pJ/Cycle respectively for 2N2P-PCG, and 2N-PCG integrated into the design. The same counterpart designed using 2-EE-SPFAL has an average energy consumption of 0.872 pJ/Cycle and 1.121 pJ/Cycle respectively with 2N2P-PCG, and 2N-PCG integrated into the design. Further, it can also be observed that for 2N-PCG integrated into the design, the 2-SPGAL based case study implementation has approximately 30% less average energy consumption (in pJ/Cycle) compared to its 2-EE-SPFAL counterpart. Thus, for 2N-PCG integration into the design, the proposed 2-SPGAL can result in more energy saving compared to 2-EE-SPFAL. On the other hand, the CMOS-based one round of PRESENT-80 encryption design has an average energy consumption of 1.611 pJ/Cycle, the highest among five different circuits compared.

Table 5.6 lists the energy-saving (in%) value in 2-SPGAL based one round

of PRESENT-80 implementation compared to its CMOS and 2-EE-SPFAL based counterpart designs. The energy-saving in 2-phase adiabatic logic are compared for the same type of PCG integrated into the design. on the other hand, the CMOS-based counterpart is implemented over DC voltage. The proposed 2-SPGAL based counterpart shows an average of 16.62% and 28.90% of energy-saving respectively with 2N2P-PCG and 2N-PCG integrated into the design, compared to its 2-EE-SPFAL counterpart. Therefore, the 2-SPGAL saves overall more energy compared to other 2-phase adiabatic logic 2-EE-SPFAL [9]. Similarly, we can see an average of 47.50% and 51.18% energy saving, with 2N-PCG and 2N2P-PCG integrated into 2-SPGAL design compared to CMOS based case-study implementation. Saving close to 50% of energy can help to increase IMD device lifetime substantially.

5.5 Energy and Security evaluation of PRESENT-80 S-box design

In Section V, the 2-SPGAL based logic gates were shown promising results for the NED, and NSD metrics. The CPA attack collects the power traces at the output of the S-box, thereby it is a vital component of the PRESENT-80 design. We implemented the S-box design using the proposed 2-SPGAL, 2-EE-SPFAL [9], and CMOS logic gates. The S-box implementation requires both ϕ_1, and ϕ_2 phases (Figure 6.8) of power clock to operate. The S-box designs using adiabatic logic were tested for two PCGs: 2N-PCG and 2N2P-PCG.

Table 5.7 shows the summary of energy consumption values and security metrics (NED and NSD) for the 2-SPGAL and 2-EE-SPFAL [9] based S-box with 2N2P-PCG and 2N-PCG integrated with the design. Similar to logic gates, we collected energy numbers for all possible input combinations for the frequency range 50 kHz to 250 kHz at 45nm technology with the load value of 10 fF. It can be observed, in Table 5.7 that energy consumption in 2-SPGAL with 2N-PCG integrated design shows superior energy consumption value, with an average value of 48.49 fJ at all frequencies in consideration. The next better energy consumption for S-box is observed for 2-SPGAL with 2N2P-PCG integrated with design with an average value of 80.18 fJ.

Figure 5.11 and 5.12 shows the comparison of NED and NSD value for S-box designed using proposed 2-SPGAL, 2-EE-SPFAL [9], and CMOS logic.

Table 5.7: Energy-efficiency and security evaluation of PRESENT-80 S-box design using 2-phase adiabatic logic.

S-box design using 2-SPGAL logic gates								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{\min}(fJ)$	80.08	50.69	78.38	47.64	78.18	46.94	77.65	45.45
$E_{\max}(fJ)$	84.09	52.57	84.51	49.67	83.00	49.04	82.49	47.64
$E_{\text{avg}}(fJ)$	81.48	51.38	80.04	48.42	79.82	47.78	79.39	46.41
NED (%)	4.78	3.59	7.25	4.08	5.81	4.27	5.86	4.60
NSD (%)	0.96	0.74	1.18	0.89	1.19	0.92	1.20	0.98
S-box design using 2-EE-SPFAL logic gates [9]								
	50 kHz		**100 kHz**		**125 kHz**		**250 kHz**	
PCG	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**	**2N2P**	**2N**
$E_{\min}(fJ)$	111.87	3654.23	106.79	1050.03	105.81	750.94	103.21	247.59
$E_{\max}(fJ)$	120.24	3971.60	114.36	1183.61	113.04	774.58	110.28	255.92
$E_{\text{avg}}(fJ)$	116.37	3898.30	110.34	1125.50	109.02	761.56	106.27	252.75
NED (%)	6.96	7.99	6.62	11.29	6.40	3.05	6.40	3.25
NSD (%)	1.28	1.45	1.31	1.83	1.30	0.82	1.30	0.82

We can see that adiabatic logic-based S-box has comparatively very low NED, and NSD value or better resilience against CPA compared to CMOS-based S-box. The S-box design using proposed 2-SPGAL, with 2N-PCG integrated into the design, shows an average of 95.86% and 99.34% better NED and NSD metric performance respectively compared its CMOS counterpart over the frequency range of 50 kHz to 250 kHz. Similarly, the 2-SPGAL S-box design with 2N2P-PCG integrated into the design shows an average of 94.07% and 99.16% better NED and NSD metric values respectively compared to CMOS counterpart over the frequency range of 50 kHz to 250 kHz. Further, the 2-SPGAL with 2N2P-PCG shows 10.15% and 12.98% better NED and NSD values respectively compared to the same counterpart implemented using 2-EE-SPFAL [9].

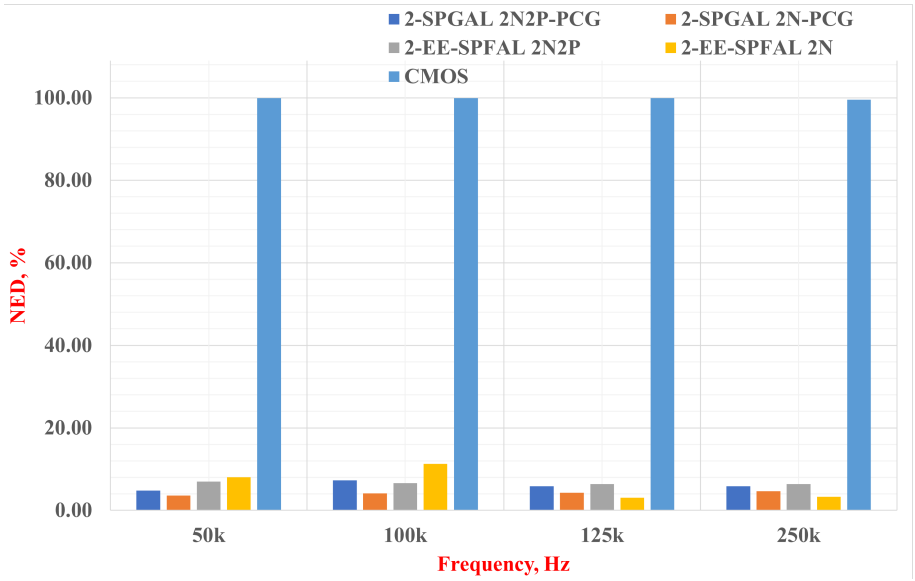

Figure 5.11: NED value comparison for PRESENT-80 S-box.

5.6 CPA Attack on one round of PRESENT-80 encryption design

The energy efficiency and security metrics comparison show the efficacy of the 2-SPGAL. It is also important to check the security resilience of the 2-SPGAL based design against power analysis attacks. The Correlation Power Analysis (CPA) is simpler to implement and has proven its success against symmetric and asymmetric encryption algorithms. The procedure to perform the CPA attack is explained in [168]. The one round of PRESENT-80 (Figure 6.8) is consist of 16 identical circuit blocks that includes four XOR gates and an S-box. Therefore, performing CPA attack on one such block would be similar to performing the CPA attack on entire circuit.

The CPA attack requires the power traces collected from the attack point. The SPICE simulation was performed with a load value 10 fF to collect the power traces. The simulation environment is noise-free and requires fewer traces for successful CPA. More power traces are needed to minimize the noise effect. The simulation environment collects 80 traces in one clock period. For CMOS-based PRESENT-80 case-study design requires 5120 traces for successful CPA. Figure 6.14 shows that key-value 14 is revealed in PRESENT-80

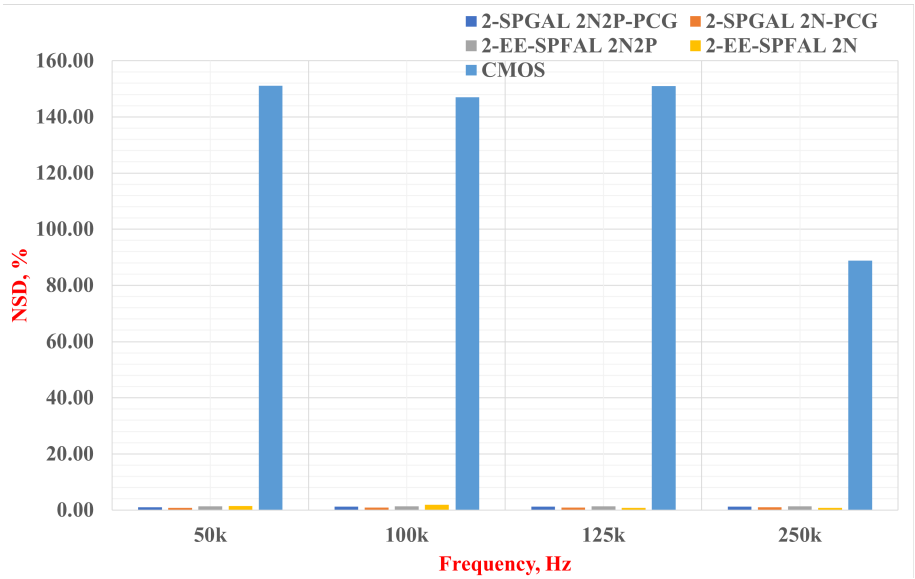

Figure 5.12: NSD value comparison for PRESENT-80 S-box.

designed using CMOS logic.

Similarly, we collected the 12,000 traces for PRESENT-80 implementation integrated with 2N-PCG and 2N-2P PCG. The larger number of traces can make the probability of CPA success higher. More traces results in a precise correlation between measured and hypothetical power traces used in the CPA attack. Figure 5.14 and 5.15 show that the correlation coefficient of actual key-value-14 is not standing out from other possible key values. The uniform current in the proposed 2-SPGAL at sinusoidal clocking helps to preserve the key. The CPA on case-study implementation shows that the proposed 2-SPGAL is energy efficient and secure against CPA attack.

5.7 Summary

This chapter presented 2-SPGAL, the 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL) for Implantable Medical Devices (IMDs). The 2-SPGAL is energy-efficient and secure against the Correlation Power Analysis (CPA) attack. The proposed 2-SPGAL was evaluated in terms of energy, and security with two synchronous resonant Power Clock Generators (PCGs): 2N-PCG, and 2N2P-PCG. The case-study

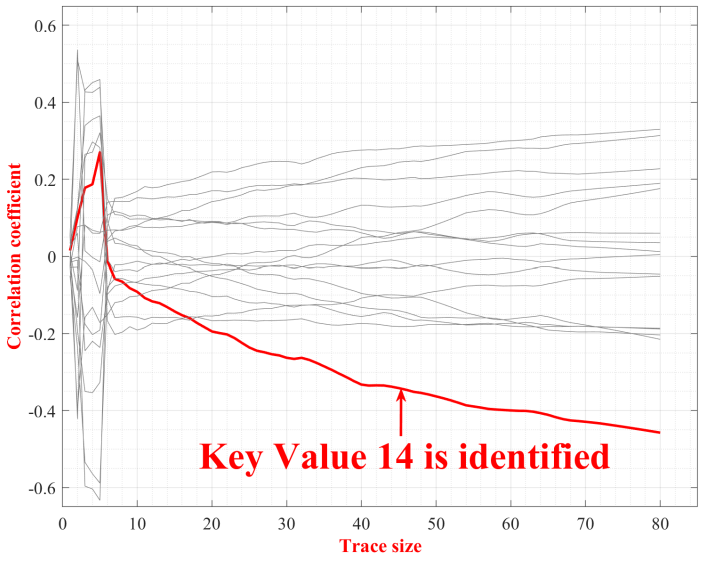

Figure 5.13: Successful Revelation of Key=14 in on one round of PRESENT-80 encryption designed with CMOS (© 2021 IEEE).

implementation of PRESENT-80 one round of encryption shows better energy saving compared to CMOS design for both 2N-PCG and 2N2P-PCG integrated with the design. The CPA attack point S-box shows better NED, and NSD as security metrics value in the proposed 2-SPGAL based design (with 2N-PCG and 2N2P PCG integrated) compared to CMOS based design. We also demonstrated that 2-SPGAL based design can protect the secret key against CPA, however, the key gets successfully revealed in CMOS based design. The proposed 2-SPGAL with its promising energy-efficient and CPA-resistant properties can be used to design energy-efficient and secure Implantable Medical Devices.

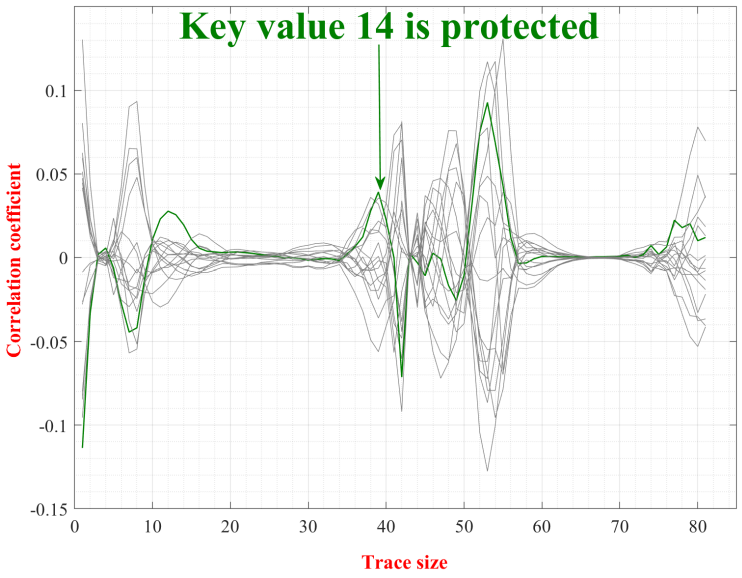

Figure 5.14: Unsuccessful CPA attack on one round of PRESENT-80 encryption designed with proposed 2-SPGAL and 2N-PCG.

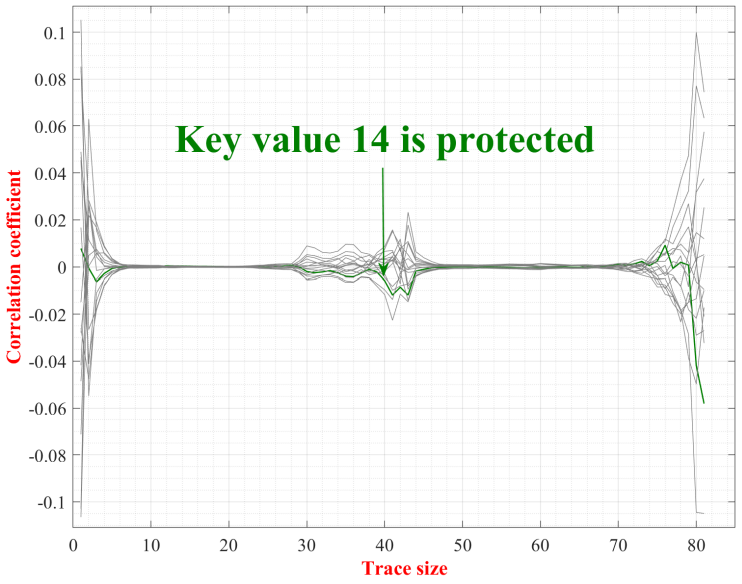

Figure 5.15: Unsuccessful CPA attack on one round of PRESENT-80 encryption design with proposed 2-SPGAL and 2N2P-PCG.

Chapter 6

2-Phase Single-Rail Clocked CMOS Adiabatic Logic (CCAL) to design secure and energy-efficient cryptographic circuits

In this work, we explore the single-rail adiabatic logic-based on 2-phase sinusoidal power clocking system. The single-rail adiabatic logic has similar logic gate structure to its CMOS counterpart. Furthermore, the single-rail adiabatic logic based cryptographic circuit are CPA resilient (similar to 2-SPGAL [53]) and reduce transistor count and saves significant energy.

The research work presented in this chapter is currently under review in [54] as A. Degada and H. Thapliyal, "Single-rail adiabatic logic for energyefficient and cpa-resistant cryptographic circuit in low-frequency medical devices," IEEE Open Journal of Nanotechnology, pp. 1-13, 2021.

6.1 Introduction

In previous chapter, we proposed two-phase sinusoidal clocking based adiabatic logic 2-phase Energy Efficient Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL) [9] and 2-phase Symmetric Pass Gate Adiabatic Logic (2-SPGAL) [10]. The above solution enables to the design of the low-energy

and CPA secure circuit. The 2-EE-SPFAL and 2-SPGAL are classified as dual-rail adiabatic logic as they produce two outputs at the logic gate, V_{out} and $\overline{V_{out}}$. The dual-rail adiabatic logic uses the two-transistor logic evaluation network to balance the switching activities, and therefore have uniform power traces. The above feature results in a larger transistor count overhead.

Currently, CMOS-based computing technology is reaching to its limit in energy efficiency with scaling down of the technology. There are two possible directions to reduce the energy consumption: (i) to reduce the energy required to distinct the logic '1' from logic '0' (ii) conserve the energy from one logical operation to the next [169] [170]. The adiabatic logic works on the energy recovery principle and is classified under the second approach mentioned above. Adiabatic logic in bulk MOSFET has emerged as an attractive choice for the designer compared to conventional CMOS due to its superior energy performance and CPA resilience.

The adiabatic logic circuits recover the energy stored inside the load capacitor (rather than dissipating as heat), thus, results in significantly low-power consumption. Further, the power traces of the adiabatic logic circuits are uniform in shape, unlike the conventional CMOS logic circuits. The uniform power traces is a very important property to disguise the processed information. The above property helps to combat the CPA. Earlier, we proposed two-phase sinusoidal clocking based adiabatic logic 2-phase Energy Efficient Secure Positive Feedback Adiabatic Logic (2-EE-SPFAL) [9] and 2-phase Symmetric Pass Gate Adiabatic Logic (2-SPGAL) [10]. The above solution enables the design of the low-energy and CPA secure circuit. The 2-EE-SPFAL and 2-SPGAL are classified as dual-rail adiabatic logic as they produce two outputs at the logic gate, V_{out} and $\overline{V_{out}}$. The dual-rail adiabatic logic uses the two-transistor logic evaluation network to balance the switching activities, and therefore have uniform power traces. The above feature results in a larger transistor count overhead.

In this research, we address the above issue by exploring the single-rail adiabatic logic called Clocked CMOS Adiabatic Logic (CCAL). The CCAL was previously proposed in [11] with preliminary analysis limited to reduction in energy consumption for logic gates and a chain of inverters. It is interesting to see the security performance of the CCAL. Further, the energy and security performance of the adiabatic logic circuits largely depends upon the Power-Clock Generator (PCG) integrated with the logic circuit. The poor interfacing suffers a reduction in energy-saving and compromised security (explained in Section II). In this article, we evaluate the energy

efficiency and security performance of the CCAL logic to design a secure cryptographic circuit with PCG integrated into the design. Further, the physiological signals in human bodies are typically a few tens to hundreds of the frequency range. In the digital domain, after sampling the operational frequencies are mostly limited up to a few kHz (Table 5.1). The adiabatic logic is saved significant energy consumption compared to its CMOS counterpart at low-frequency applications. Some example of the low-frequency medical device includes inductive implants, bioimpedance meter, Electrical Impedance Myography (EIM), hearing aids, Electrical Impedance Tomography (EIT), Magnetic Particle Imaging (MPI), and Body-Coupled Communication (BCC), etc. In this article, we evaluate the performance of the CCAL based cryptographic circuit for the frequency range of 50 kHz to 250 kHz.

6.1.1 Key Contribution

The key contributions of this work are as follows:

- The article explores CCAL, a novel single-rail Clocked CMOS Adiabatic Logic (CCAL) to design energy-efficient and secure cryptographic circuits. The CCAL can be an alternate choice for low-energy and CPA-resistant medical devices.

- The case-study implementation of PRESENT-80 S-Box circuitry saves more than 95% energy for frequency range 50 kHz to 125 kHz and approximately 60% more energy saving at 250 kHz compared to its CMOS counterpart. The above energy saving can be highly beneficial to design low-power cryptographic circuits.

- The case-study implementation shows saving of 45.74% and 34.88% of transistors compared to 2-EE-SPFAL [9] and 2-SPGAL [10]. At 250 kHz, compared to the dual-rail adiabatic designs of S-box based on 2-EE-SPFAL and 2-SPGAL, the CCAL based S-box shows 32.67% and 11.21% of energy savings, respectively. Thus, CCAL can be an alternate choice to design a secure and energy-efficient cryptographic circuit with lesser transistor overhead compared to its dual-rail adiabatic logic counterpart.

- We also presents the effect of varying tank capacitance in 2N2P-PCG over energy efficiency and security performance. We demonstrate that

having 200 fF value of tank capacitor (C_E) in 2N2P-PCG can provide optimum energy and security features.

- The single-rail CCAL based circuitry removes the need for discharge circuitry required in its dual-rail counterpart. It helps to reduce the external need for the control signals for discharge circuitry.
- We demonstrate that the PRESENT-80 using CCAL can successfully defend the encryption key against the CPA attack for both 2N2P-PCG integrated into the design. However, the encryption key is revealed in the same counterpart design using CMOS.

6.2 Clocked CMOS Adiabatic Logic (CCAL)

In recent years, researchers have shown the effectiveness of power-analysis attacks to reveal the encryption key in cryptographic circuits. There have been many countermeasures are proposed, e.g., masking [91], random instruction injection [92], non-deterministic processors [93], random register renaming [94], secure co-processors [95], and cell-level countermeasures [96]. In this work, we employ the cell-level countermeasure, i.e. to build secure logic gates. Adiabatic logic design is one such approach, that can thwart the power-analysis attacks such as CPA.

In this section, we briefly discuss the adiabatic logic and the common metrics used to evaluate CPA resilience. Further, the energy and security performance of adiabatic logic circuits largely depend on the Power-Clock Generator (PCG) integrated into the design. We also provide a brief overview of the type of the PCG integrated with design.

6.3 Evaluation in Energy-efficiency and Security Metrics performance evaluation of the CCAL

In this section, we will first illustrate the background on the logic gate structure of CCAL. Then, we will present the energy efficiency and security performance evaluation of CCAL logic gates with 2N2P-PCG integrated into the design.

6.3.1 Background on CCAL

The Clocked CMOS Adiabatic Logic (CCAL) was previously proposed in [11] with preliminary analysis limited to reduction in energy consumption for logic gates and a chain of inverters. Figure 6.1 shows the generalized gate structure of CCAL. It consists of two primary parts, (i) CMOS logic (ii) clock connection which connects CMOS logic to the sinusoidal clocking part. The signals VPC and $\overline{VPC}$ are two out-of-phase sinusoidal power clocks. The operation of CCAL can be explained in two stages: (i) Evaluation (E) (ii) Recovery (R). During the Evaluation stage, when the voltage at both clock signals is more than the threshold voltage (V_{th}) then it turns on both transistor M1 and M2 (clock connection network). Then the PMOS and NMOS blocks evaluate the output logic based on the input signal logic. During the Recovery (R) phase, the output voltage stored in load capacitance is held until the next evaluation phase.

There have been many low-energy solutions in the research literature that works low-frequency operation. The adiabatic circuit-based cryptographic circuits are found to defend encryption keys against power-analysis attacks. Earlier, we proposed the two-phase sinusoidal clocking-based dual-rail adiabatic logic 2-SPGAL[10] and 2-EE-SPFAL [9]. The CCAL can be an alternate choice to design CPA secure and energy-efficient cryptographic circuits. The single-rail adiabatic, e.g. CCAL has less logic overhead compared to its dual-rail adiabatic logic counterpart. The above properties can be highly beneficial for resource-constrained IMDs. Further, the dual-rail logic, 2-EE-SPFAL [9] and 2-SPGAL [10] requires the additional discharge circuitry and corresponding control signals. The CCAL network removes the need for discharge circuitry and the logic gate structure is very similar to the CMOS logic gate.

However, the performance of the adiabatic logic is largely affected by the integration of the PCG. It is important to investigate the performance of the CCAL based cryptographic circuits energy efficiency and security performance with the integration of PCG in design. Therefore, we evaluated the performance of the CCAL based circuits with 2N2P-PCG integrated into the design.

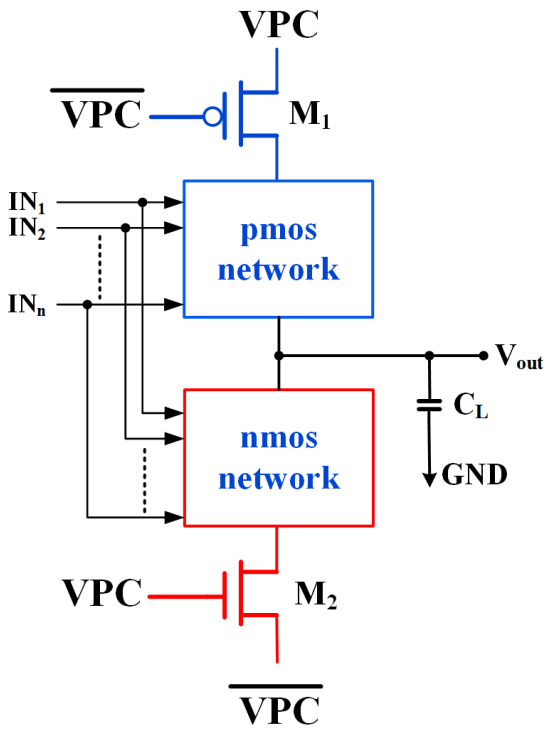

Figure 6.1: Clocked CMOS Adiabatic Logic (CCAL) gate schematic [11].

6.3.2 Energy-efficiency and security evaluation of CCAL logic gates

Logic gates are the primary constituent of a larger circuit. It becomes important to check the energy and security metrics performance to build low-energy and secure cryptographic circuits. In this section, we explain the energy-efficiency and security performance of the CCAL logic gates. We have compared the simulation results of the CCAL logic gate with CMOS, 2-EE-SPFAL [9], and 2-SPGAL [10] logic gates.

The energy consumption in medical devices should be as minimal as possible. Further, to build a secure circuit the variation in energy consumption for input combination variation should be ideally zero. The CPA calculates the correlation between hypothetical power traces of all possible keys and collected power traces from the circuit. Uniform power traces disguise the linear dependency. To look at this feature at the circuit level, we check the

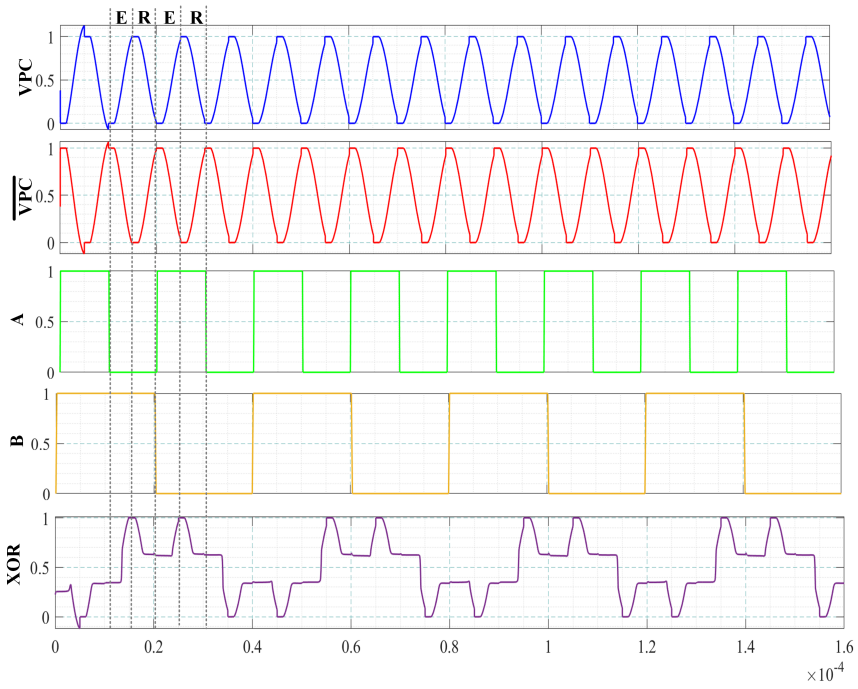

Figure 6.2: CCAL-based XOR logic gate waveform with 2N2P-PCG integrated into the design.

energy performance of the logic gate at all possible change in input values.

$$E = \int_0^T V_P I_P dt \tag{6.1}$$

The energy consumption is the integration of the product of voltage (V_p) and current (I_p), i.e. power consumption for input signal [167]. We built CCAL logic gates using 45nm technology and considered the load of 10 fF. Further, the energy and security performance of adiabatic logic circuits largely depends upon the PCG integrated into the design. Therefore, the energy and security metric performance was evaluated for logic gates with 2N2P-PCG integrated into the design. We target particularly low-frequency medical device encryption, therefore, the frequency range of 50 kHz to 250 kHz is considered.

The variation in energy consumption value provides more insight than observing the current traces. We used SPICE simulation to collect energy consumption value for a total of 2^{2n} possible cyclic variations in the n-bit circuit. The energy consumption values can be used in Equation 2.7 and 2.8 equation to calculated NED and NSD value. For ideal conditions, equal energy consumption results in zero NED and NSD values. However, for practical scenarios, the NED and NSD value should be as low as possible. Having lower NED and NSD value results in less correlation between hypothetical and actual power traces. Thus, the circuit can protect the stored encryption key.

It is very important to observe the energy saving in CCAL compared to other logic gates. For equal comparision, the dual rail logic circuits 2-EE-SPFAL [9] and 2-SPGAL [10] are designed with 2N2P-PCG integrated into the design, similar to the CCAL counterpart. For the energy performance metric, we have listed E_min, E_max and E_avg. A smaller difference between E_min, and E_max indicates the energy consumption across all possible input combinations is smaller and results in a better secure circuit. Further, the E_avg for each logic gate should be as low as possible for better energy efficiency.

Table 6.1 shows the comparison of CCAL AND logic gate with its counterpart in CMOS, 2-EE-SPFAL [9], and 2-SPGAL [10]. The CCAL AND logic gate has the lowest E_avg value for the frequency range of 50 kHz to 250 kHz. The CCAL AND logic gate has on an average of 4.7248 fJ E_avg for the frequency range of 50 kHz to 250 kHz. While in its CMOS, 2-EE-SPFAL

Table 6.1: Energy-efficiency and security performance comparison for AND logic gate.

	50 kHz				100 kHz			
Metric	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL** [10]	**CCAL**	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL** [10]	**CCAL**
$E_{\min}(fJ)$	0.3745	11.8596	9.1762	4.8398	0.1873	11.7577	11.1575	4.5769
$E_{\max}(fJ)$	38.0678	12.1081	9.2971	5.3530	29.8538	11.9808	11.3861	5.1297
$E_{\text{avg}}(fJ)$	9.8487	12.0227	9.2425	4.9780	7.6402	11.8864	11.2964	4.7216
NED (%)	99.02	2.05	1.30	9.59	99.37	1.86	2.01	10.78
NSD (%)	117.08	0.60	0.40	3.55	118.71	0.57	0.58	4.24
	125 kHz				**250 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL**[10]	**CCAL**	**CMOS**	**2-EE-SPFAL**[9]	**2-SPGAL**[10]	**CCAL**
$E_{\min}(fJ)$	0.1498	11.7009	11.1185	4.5224	0.0749	11.7677	11.1600	4.3702
$E_{\max}(fJ)$	28.2615	11.9486	11.3740	5.0853	25.1593	12.0363	11.4598	4.9547
$E_{\text{avg}}(fJ)$	7.2078	11.8591	11.2804	4.6682	6.3756	11.9351	11.3488	4.5316
NED (%)	99.47	2.07	2.25	11.07	99.70	2.23	2.62	11.80
NSD (%)	119.18	0.59	0.67	4.42	120.26	0.65	0.78	4.66

[9], and 2-SPGAL [10] counterpart the average of E_{avg} is 7.7681 fJ, 11.9258 fJ, and 10.7920 fJ. Therefore, we can conclude that the sinusoidal clocking circuits on top of the PMOS and NMOS network help to reduce significant energy consumption compared to conventional CMOS logic and also to its dual-rail adiabatic logic counterpart. Table 6.2 summarizes the average energy saving (in %) in CCAL-based AND logic gate compared to its CMOS, 2-EE-SPFAL [9], and 2-SPGAL [10] counterpart.

Table 6.2: E_{avg} - Energy saving (in %) in CCAL AND logic gate.

Type of the logic	**Baseline Logic to compare**	**50 kHz**	**100 kHz**	**125 kHz**	**250 kHz**
Dual-Rail Adiabatic	2-EE-SPFAL [9]	58.60	60.28	60.64	62.03
	2-SPGAL [10]	46.14	58.20	58.62	60.07
Single-Rail	Conventional CMOS	49.46	38.20	35.23	28.92

For the secure encryption circuit design, it becomes important to check the NED and NSD performance of the logic gate before building the larger circuits. In this work, we primarily compared the NED and NSD value of CCAL logic gates with their CMOS counterpart. The CMOS circuit is considered the benchmark because has been shown to be vulnerable to CPA attacks. Figure 6.3 and 6.4 shows the comparison of NED and NSD security performance metrics for CCAL and CMOS AND logic gate. We can see that CCAL AND logic gate has a significantly smaller value of NED and NSD compared to CMOS AND logic. The average NED value for CCAL AND

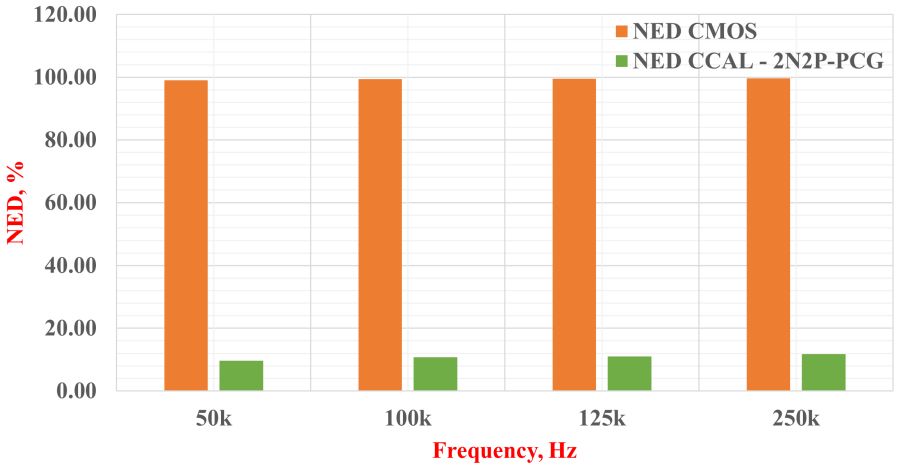

Figure 6.3: NED value comparison for AND logic gate.

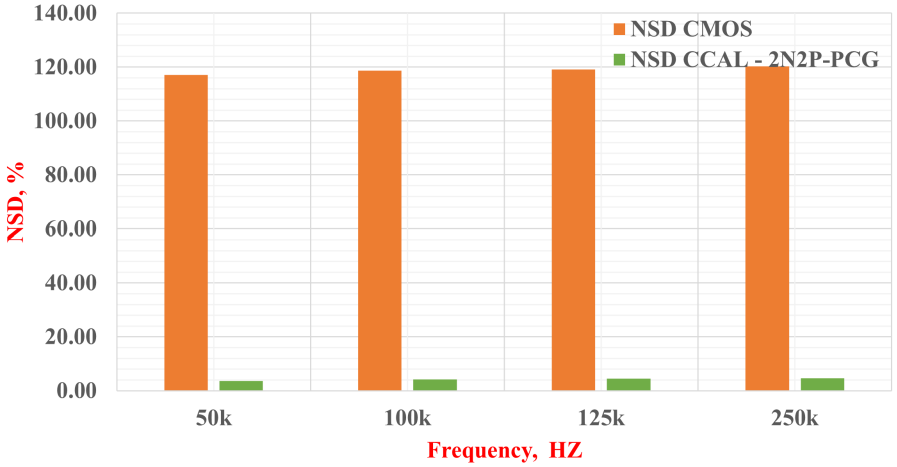

Figure 6.4: NSD value comparison for AND logic gate.

logic gate is 10.81% compared to 99.39% in its CMOS counterpart for the frequency range of 50 kHz to 250 kHz. This results in 89.13% better NED value in CCAL AND logic. Similarly, we can see an average of 96.45% better NSD value in CCAL AND logic gate compared to its CMOS counterpart in the same frequency range.

Table 6.3: Energy-efficiency and security performance comparison for XOR logic gate.

	50 kHz				**100 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL** [10]	**CCAL**	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL** [10]	**CCAL**
$E_{\min}(fJ)$	0.2459	11.7161	11.1072	5.5896	0.1529	11.5779	11.0179	5.3592
$E_{\max}(fJ)$	32.5163	11.7165	11.1077	5.6366	25.9986	11.5783	11.0184	5.3926
$E_{\text{avg}}(fJ)$	16.3697	11.7163	11.1075	5.6114	13.0968	11.5781	11.0181	5.3775
NED (%)	99.244	0.003	0.004	0.833	99.412	0.004	0.004	0.619
NSD (%)	69.537	0.001	0.002	0.284	69.671	0.002	0.002	0.210
	125 kHz				**250 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL**[10]	**CCAL**	**CMOS**	**2-EE-SPFAL**[9]	**2-SPGAL**[10]	**CCAL**
$E_{\min}(fJ)$	0.1250	11.5692	10.9915	5.3095	0.0919	11.6306	11.0635	5.2555
$E_{\max}(fJ)$	22.8099	11.5698	10.9921	5.3643	22.7796	11.6313	11.0642	5.2870
$E_{\text{avg}}(fJ)$	11.4741	11.5695	10.9918	5.3405	11.4466	11.6309	11.0638	5.2711
NED (%)	99.452	0.005	0.006	1.1023	99.597	0.006	0.007	0.595
NSD (%)	69.752	0.003	0.003	0.389	69.906	0.003	0.003	0.206

Table 6.4: E_{avg} - Energy saving (in %) in CCAL XOR logic gate.

Type of the logic	**Baseline Logic to compare**	**50 kHz**	**100 kHz**	**125 kHz**	**250 kHz**
Dual-Rail Adiabatic	2-EE-SPFAL [9]	52.11	53.55	53.84	54.68
	2-SPGAL [10]	49.48	51.19	51.41	52.36
Single-Rail	Conventional CMOS	65.72	58.94	53.46	53.95

Similar to the AND logic gate, we repeated the simulation experiment for the XOR logic gates for all four logic designs in consideration. Table 6.3 lists the summary of simulation results for the XOR logic gate for the frequency range of 50 kHz to 250 kHz. We can see in Table 6.3 that the CCAL XOR logic gate has superior energy performance results. The average of $_{\text{avg}}$ value, for the frequency range of 50 kHz to 250 kHz, in the CCAL XOR logic gate is 5.40 fJ. However, in the same CMOS, 2-EE-SPFAL [9], and 2-SPGAL [10] counterparts have an average of $_{\text{avg}}$ values are 13.0968 fJ, 11.6237 fJ, and 11.0453 fJ. Table 6.4 saving lists the energy saving in CCAL XOR logic gate compared to single-rail counterpart, CMOS, and dual-rail adiabatic logic counterpart 22-EE-SPFAL [9], and 2-SPGAL [10]. The

CCAL XOR logic gate saves on an average more than 58% energy compared to CMOS, and 53% and 51% more energy saving compared to 2-EE-SPFAL [9], and 2-SPGAL [10] based XOR gate respectively.

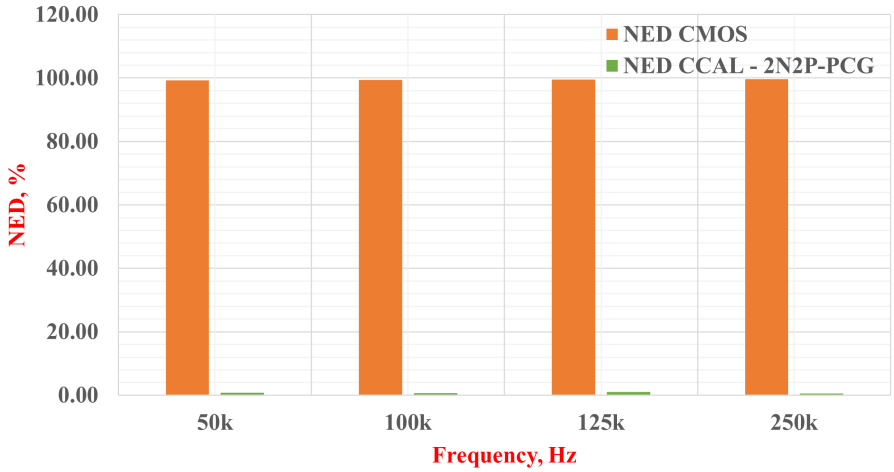

Figure 6.5: NED value comparison for XOR logic gate.

Figure 6.5 and 6.6 graphically show the comparison of NED and NSD security metric performance for CCAL and CMOS XOR logic gate. Similar to the AND logic gate, the CCAL based XOR logic gate is superior in NED and NSD security metric performance. The CCAL XOR logic gate has an average of 99.23% better NED value compared to the CMOS XOR logic gate over the frequency range of 50 kHz and 250 kHz. Further, an average of 99.61% better NSD value is noted for the CCAL XOR logic gate compared to its CMOS counterpart in the same frequency range.

Figure 6.7 helps to understand the relation between the E_{avg} and supply voltage at frequency value 100 kHz, for CCAL-based XOR logic gate, with 2N2P-PCG integrated into the design. We also plotted the corresponding NED and NSD value along with E_{avg} on the same graph. We see that E_{avg} is decreasing with lowering the supply voltage. However, the security performance metric NED and NSD are higher with low supply voltage. The CCAL-based XOR logic gate shows better security performance as the supply voltage reaches a higher value. The better security performance is attributed to the minimum deviation in energy number.

It is important to note that NED and NSD values in CCAL logic gates are relatively better in dual-rail adiabatic logic (2-EE-SPFAL [9], and 2-

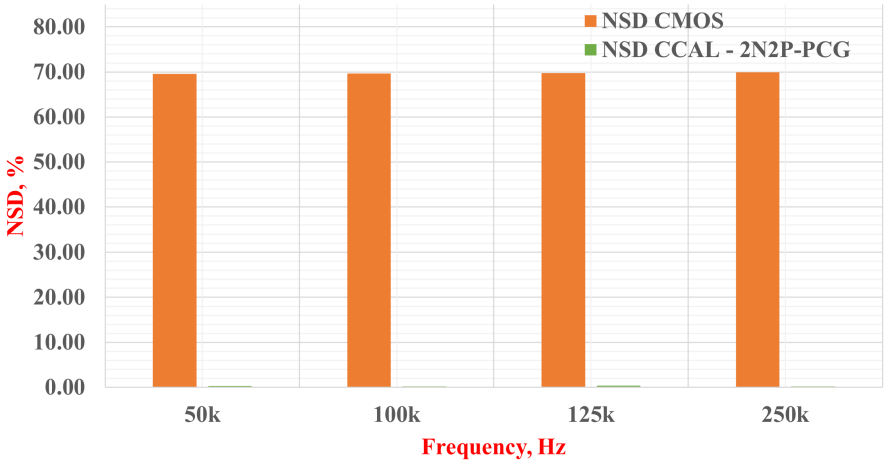

Figure 6.6: NSD value comparison for XOR logic gate.

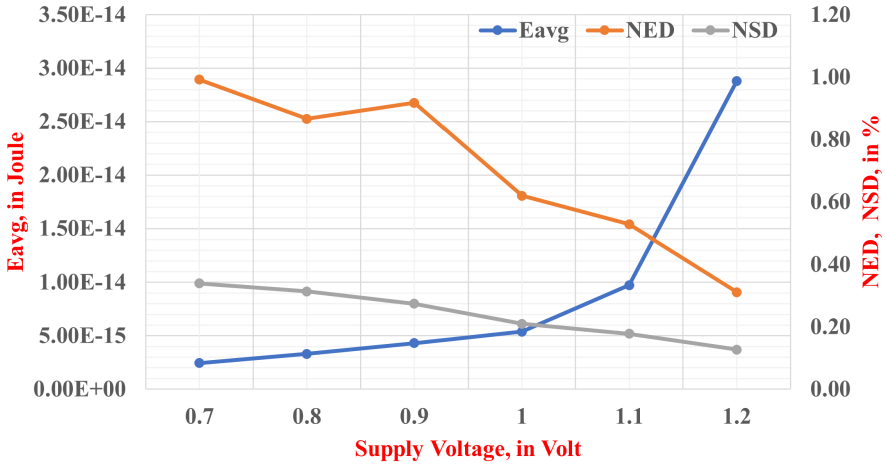

Figure 6.7: E_{avg}, NED and NSD metric in CCAL-based XOR logic gate as a function of the supply voltage.

SPGAL [10]) compared to single-rail adiabatic logic CCAL. This is expected behavior as dual-rail circuit uses two balanced switching logic evaluation networks F and $\overline{F}$. The switching in the evaluation block happens in a complementary fashion. Thus, the more uniformity in current results in logic gate output. However, for practical side-channel attacks (e.g. CPA in our case), it becomes important to check whether the CCAL based encryption circuit can prevent the revelation of the encryption key. The later part of the paper explains the CPA attack performance results over CCAL logic-based case-study implementation of the lightweight cryptographic cipher.

6.4 A Cryptographic Circuit Case-Study: PRESENT-80 S-box

In this section, first, we provide background information on lightweight cryptographic cipher PRESENT. The Substitution-box (S-box) is a vital component in the PRESENT cipher. We use the S-box as case-study implementation and show the comparison of transistor count implementation in adiabatic logic CCAL, 2-EESPFAL [9] and 2-SPGAL [10]. We also provide energy and security metric performance of the case-study design with 2N2P-PCG integrated into the design.

6.4.1 Importance of S-box in PRESENT-80

The cryptographic cipher used in medical devices should be low-power and lightweight as they run on battery and have limited silicon space. PRESENT is one such popular lightweight cryptographic cipher [5]. Further, the counter mode operation in the PRESENT makes it suitable in challenge-response authentication [166]. The PRESENT comes in two variants based on the key size, 80-bit or 120-bit. The PRESENT-80, is an 80-bit key variant with a total of 32 rounds of encryption. In PRESENT-80, the first 31 rounds of encryption are identical and its schematic is shown in Figure 6.8.

The PRESENT-80 has three fundamental operations. First, the plain text is XORed with 64 bits of the key. During the second operation, the Substitution-box (S-box) does a non-linear transformation of the 4-bit blocks, with a total of 16 such operations happening in parallel. The last operation is the permutation of S-box output to create further randomization. The S-box is the key constituent of PRESENT-80. Therefore, in this work, we have

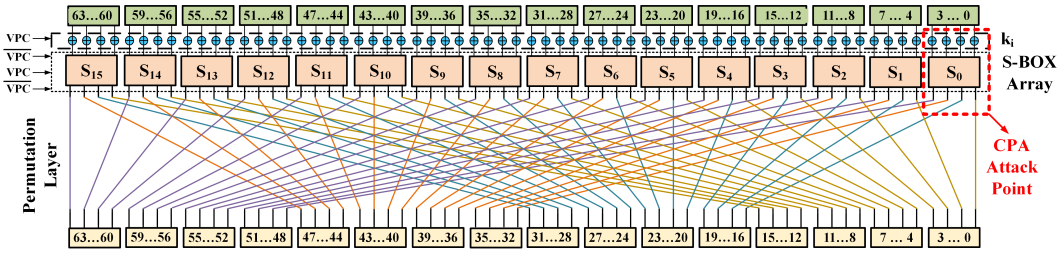

Figure 6.8: one round of PRESENT-80 implementation using 2-phase adiabatic logic [10] (© 2021 IEEE).

evaluated the transistor counts, energy efficiency, and security metrics performance comparison for S-box for 2-EE-SPFAL [9], 2-SPGAL [10], CCAL, and CMOS.

6.4.2 Transistor Count Saving analysis in CCAL-based case-study implementation of PRESENT- 80 S-box

We can see from Figure 6.8 that S-box is a critical part of the PRESENT-80 implementation. In this section, we explain the S-box circuit implementation using four different logic circuits, i.e. 2-EE-SPFAL [9], 2-SPGAL [10], CCAL, and CMOS.

Table 6.5: Transistor count in PRESENT-80 S-box designed using dual-rail logic.

Logic Gates	**Number of Logic Gates**	**Total Transistor Counts**	
		2-EE-SPFAL [9]	**2-SPGAL** [10]
Buffer	12	96	72
AND	16	224	192
OR	8	112	96
XOR	7	84	70

Table 6.5 illustrates the number of the transistors required to implement PRESENT-80 S-box using dual-rail adiabatic logic. The dual-rail adiabatic logic inherently works in pipeline fashion. In other words, the successive

blocks of the circuits operate on different phases. In case of 2-phase clock, they are in-phase and out-of-phase [9] [10]. In order to make the output appear on the same clock phase, we need to put extra buffers for synchronization.

Table 6.6: Transistor count in PRESENT-80 S-box designed using single-rail logic.

Logic Gates	**Number of Logic Gates**	**Total Transistor Counts**	
		CCAL	**CMOS**
AND	16	128	96
OR	8	64	48
XOR	4	40	32
XNOR	4	48	40

Table 6.6 represents the number of logic gates and transistor count for PRESENT-80 S-box implemented using single-phase logic. The PRESENT-80 S-box implementation using CCAL is similar to CMOS-based implementation, except it requires two complementary sinusoidal power clocks and two extra transistors for clocking circuitry on top of the logic evaluation network. In the previous section, we have seen that the CCAL logic gates require significantly less energy consumption, as well as improve the resilience against the CPA attack.

Table 6.7: Transistor count comparison for CCAL, 2-EE-SPFAL [9], 2-SPGAL [10] and conventional CMOS for PRESENT-80 S-box design.

Logic	**Number of Transistors**	**Overhead compared to CMOS, in %**	**Transistor Saving in CCAL, in %**
2-EE-SPFAL [9]	516	138.89	**45.74**
2-SPGAL [10]	430	99.07	**34.88**
CCAL	280	29.63	–
CMOS	216	–	–

Table 6.7 presents the comparison of the number of transistors required to implement PRESENT-80 S-box for different logic. The dual-rail adiabatic logic has more balanced switching activities, thus resulting in a more secure

structure against CPA. However, the inherent structure of dual-rail logic results in more transistor counts. The transistor count overhead in 2-EE-SPFAL [9], and 2-SPGAL [10] compared to their CMOS-based S-box counterpart is approximately 139% and 99% respectively. On the other hand, the transistor overhead in CCAL based CMOS is 29.63%. Further, the CCAL based S-box implementation saves 34.88% and 45.74% of transistor count compared to dual-rail logic 2-EE-SPFAL [9], and 2-SPGAL [10] respectively. For the space-limited IoT structure, the CCAL logic presents an alternative to design secure cryptographic circuits with less transistor overhead.

6.4.3 Energy and Security Performance Evaluation of Case-Study Design PRESENT-80 S-Box

The CCAL based logic gates shows promising results for the NED, and NSD metrics. The CPA attack collects the power traces at the output of the S-box, thereby it is a vital component of the PRESENT-80 design. We implemented the S-Box design using the proposed CCAL and CMOS logic gates. The S-Box implementation requires both VPC and $\overline{VPC}$ phases (Figure 6.8) of power clock to operate. The S-box designs using adiabatic logic were tested with 2N2P-PCG.

Table 6.8 lists the energy-efficiency performance and calculated NED and NSD metrics. The energy consumption for adiabatic circuits was calculated for 2N2P-PCG integrated into the design. Similar to the logic gates, we collected the energy number in SPICE simulation for the frequency range 50 kHz to 250 kHz. The PRESENT-80 S-box circuit was designed at 45 nm technology and the load value was considered 10 fF. We can see in Table 6.8 that CCAL based S-box shows better energy performance than CMOS, 2-EE-SPFAL [9] and 2-SPGAL [10] over frequency range 50 kHz to 250 kHz. The average of E_{avg} for CCAL based S-box is 74.23 fJ for the frequency range 50 kHz to 250 kHz. For the same frequency range, the average of E_{avg} in CMOS, 2-EE-SPFAL [9] and 2-SPGAL [10] is approximately 1981 fJ, 110 fJ and 80 fJ respectively. Therefore, adding a clocking network on top of the pmos and nmos circuit helps to reduce the energy consumption value.

Similar to logic gate, it is interesting to see the NED and NSD performance between CCAL and CMOS. Figure 6.9 and 6.10 shows graphical comparison for NED and NSD values in CCAL and CMOS for S-box circuit. The NED and NSD values in CCAL based PRESENT-80 S-box is overall lower

Table 6.8: Energy-efficiency and security performance comparison for PRESENT-80 S-Box.

	50 kHz				100 kHz			
Metric	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL** [10]	**CCAL**	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL** [10]	**CCAL**
E_{min} (fJ)	16.10	111.87	80.08	72.13	8.05	106.80	78.38	68.41
E_{max} (fJ)	24427.77	120.24	84.09	82.20	13822.58	114.36	84.51	78.10
E_{avg} (fJ)	3713.30	116.37	81.48	78.58	2251.87	110.34	80.04	74.46
NED (%)	99.93	6.96	4.78	12.24	99.94	6.62	7.25	12.41
NSD (%)	151.09	1.28	0.96	2.07	147.00	1.31	1.18	2.10
	125 kHz				**250 kHz**			
Metric	**CMOS**	**2-EE-SPFAL** [9]	**2-SPGAL**[10]	**CCAL**	**CMOS**	**2-EE-SPFAL**[9]	**2-SPGAL**[10]	**CCAL**
E_{min} (fJ)	6.44	105.81	78.18	67.32	3.22	103.22	77.65	64.20
E_{max} (fJ)	11375.77	113.03	83.00	76.89	709.64	110.28	82.49	73.72
E_{avg} (fJ)	1785.21	109.02	79.83	73.38	175.74	106.27	79.39	70.49
NED (%)	99.94	6.40	5.81	12.45	99.55	6.40	5.86	12.90
NSD (%)	151.00	1.30	1.19	2.11	88.77	1.30	1.20	2.19

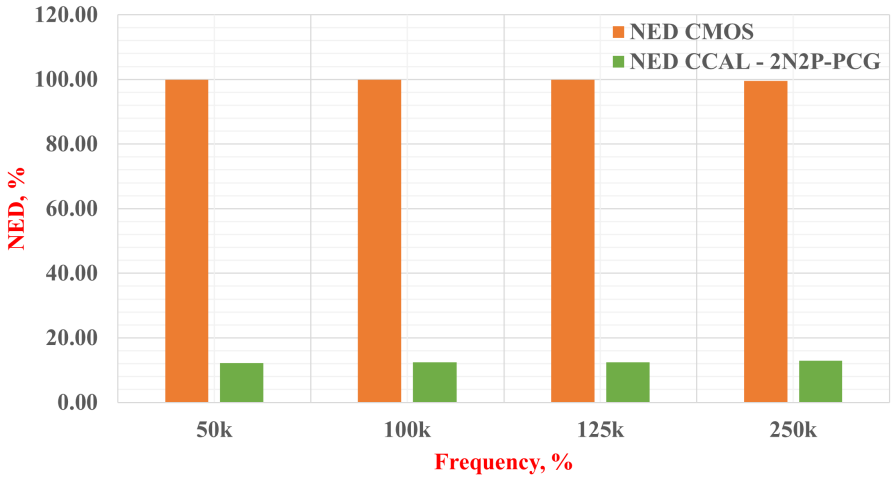

Figure 6.9: NED value comparison for PRESENT-80 S-box.

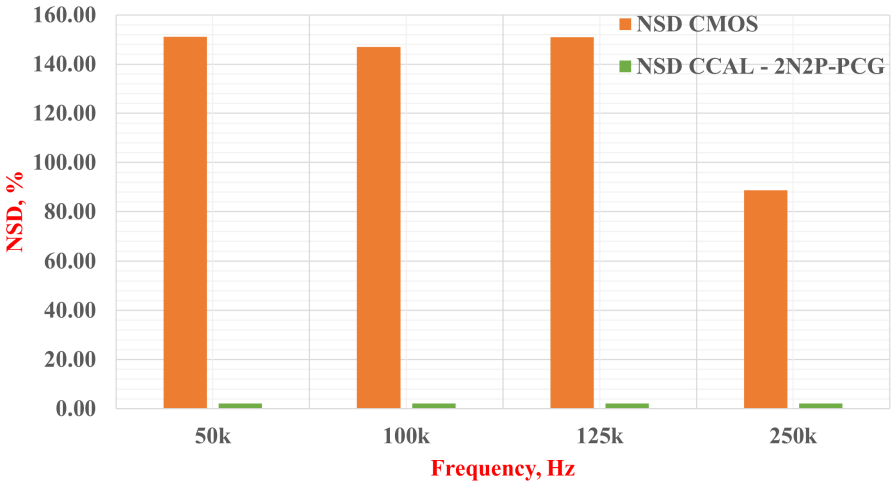

Figure 6.10: NSD value comparison for PRESENT-80 S-box.

for the frequency range 50 kHz to 250 kHz. The average NED value for the CCAL S-box is 12.50%, while in CMOS S-box it is 99.84% over frequency range 50 kHz to 250 kHz. The CCAL based S-box shows overall 97.48% improvement in NED security metric. Similarly, the NSD performance in CCAL-based S-box is average of 2.12% over frequency range 50 kHz to 250 kHz. For same frequency range, CMOS-based S-box have an average NSD value 134.46%. The CCAL-based S-box have overall 98.43% better NSD performance for frequency range 50 kHz to 250 kHz.

Table 6.9: E_{avg} - Energy saving (in %) in CCAL based PRESENT-80 S-Box.

Type of the logic	**Baseline Logic to compare**	**50 kHz**	**100 kHz**	**125 kHz**	**250 kHz**
Dual-Rail Adiabatic	2-EE-SPFAL [9]	32.47	32.52	32.70	32.67
	2-SPGAL [10]	3.56	6.97	8.08	11.21
Single-Rail	Conventional CMOS	97.88	96.69	95.89	59.89

The CCAL-based S-box shows better security metric performance compared to its CMOS counterpart. We can see that CCAL-based S-box has better energy-efficiency performance compared to its dual-rail adiabatic counterpart. However, the dual-rail adiabatic logic, 2-EE-SPFAL [9] and 2-SPGAL [10] have better NED and NSD performance. The better security performance in dual-rail logic is an attribute of the balance switching activities in logic evaluation network. However, the CCAL has significant security per-

formance improvement compared to CMOS. It will be interesting to see the performance of the CCAL based circuit against the CPA attack (explained in the next section).

6.5 Effect of varying capacitor and inductor in LC tank in 2N2P-PCG for energy efficiency and security performance analysis in case-study

$$Q = 2\pi \frac{\text{Maximum Energy Stored}}{\text{Energy Dissipated per Cycle}} \tag{6.2}$$

The Q factor is a key factor in the power analysis of the RLC resonator circuit. When the adiabatic circuit is integrated with 2N2P-PCG (Figure 2.7) then it can be modeled as an RLC circuit. Equation 6.2 shows the relation between the Q factor and average power dissipation. We need a larger Q factor in order to have minimum power dissipation. However, in the RLC circuit, the Q factor of the LC tank circuit depends upon the Q factor of inductor and capacitor with their parasitic resistance [171].

$$Q_{\text{tank}} = \omega_0 C \left(R_L \| R_C\right) = Q_L \| Q_C \tag{6.3}$$

Equation 6.3 shows the dependence of the Q factor of 2N2P-PCG tank circuit on Q factor of inductor ($Q_L = \frac{R_L}{\omega_0 L}$) and capacitor ($Q_C = \omega_0 C R_C$) respectively. In the above equations, R_L is the parasitic resistance of the inductor, and R_C is the parasitic resistance of the capacitor [171]. Therefore, we hypothesize that there will be a certain value of the inductor and capacitor for which the Q factor is maximum. Higher Q can result in lower energy dissipation. Further, it will also be interesting to see the effect on security performance metrics.

To check our hypothesis, we fixed the frequency value to 100 kHz. We calculated the different combinations of L and C (Equation 2.2) for the frequency 100 kHz. Similar to the logic gate energy and security experiment, we collected energy consumption values for a total of 256 cyclic combinations of the inputs in CCAL-based S-box circuitry. Figure 6.11 shows the E_{avg} at different capacitive value in LC tank circuit in 2N2P-PCG circuit. We can see that the lowest E_{avg} value of 74.46 fJ at capacitor value 100 fF.

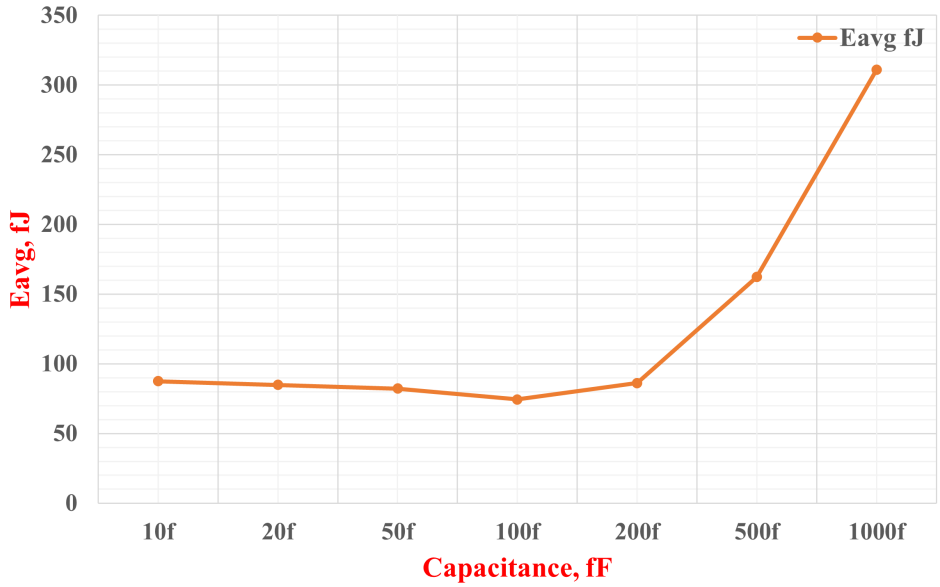

Figure 6.11: Effect of varying capacitor and inductor values over Average energy consumption in PRESENT-80 S-box.

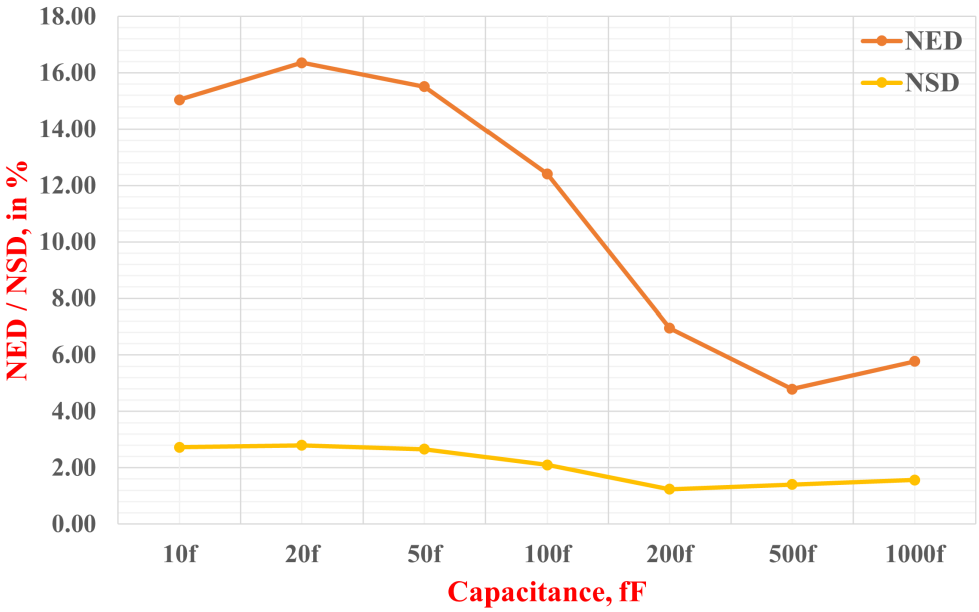

Figure 6.12: Effect of varying capacitor and inductor values over NED and NSD in PRESENT-80 S-box.

Further, we can also observe the effect on security performance metrics NED and NSD. Figure 6.12 shows the change in NED and NSD values at different values of the capacitors. The lowest NED and NSD values are observed are 4.79% and 1.40% at capacitor value 500 fF. The graph in Figure 6.12 helps to understand the capability of the circuit to thwart the Correlation Power Analysis (CPA) attack. The lowest value of NED and NSD indicates that the circuit is more robust against CPA at 500 fF capacitance value in 2N2P-PCG.

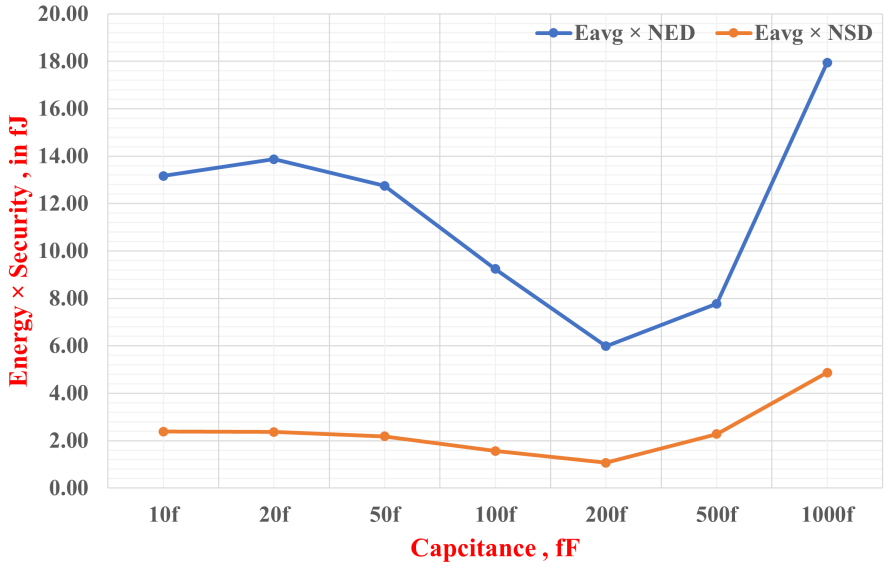

Figure 6.13: Energy-security trade-off in PRESENT-80 S-box designed using CCAL.

We define the energy-security trade-off product as $Energy \times Security$ and measure in Joule. Previously, we have seen that the energy and security metrics performance shows the different trend for PCG tank capacitor C_E values. The case-study implementation shows optimum energy performance for C_E value of 100 fF and security performance at 500 fF. For optimum energy and security performance, the trade-off product $Energy \times Security$ should be minimum. Figure 6.13 shows an insight for the energy and security performance metrics together at different tank capacitor values. We can see that for capacitor value 200 fF has the lowest $E_{avg} \times NED$ and $E_{avg} \times NSD$ equal to $5.98fJ$ and $1.07fJ$ respectively. Thus, we can say that having 200

fF value of tank capacitor (C_E) in 2N2P-PCG can provide optimum energy and security performance together.

6.6 CPA attack simulation

In the previous section, we demonstrated the efficacy of the CCAL to design low-energy and CPA resilient cryptographic circuits. The CCAL based S-box was energy efficient, however, the NED and NSD performance were relatively higher compared to Dual-Rail adiabatic logics 2-EE-SPFAL [9] and 2-SPGAL [10]. In this section, we subject the CCAL based S-box design against the CPA. The article [168] illustrates the procedure to carry out the CPA in SPICE simulation. We can see in Figure 6.8 that one round of PRESENT-80 encryption contains 16 identical blocks. Each block has four XOR logic gates and a non-linear transformation circuit, called S-box. Therefore, the output of S-box is considered as CPA attack point in the literature [10], [9], [6].

The CPA attack requires the power traces collected from the attack point. The SPICE simulation was performed with a load value of 10 fF to collect the power traces. The simulation environment is noise-free and requires fewer traces for successful CPA. If a CPA attack is carried out in a noisy environment then it requires a larger number of traces. We collected power traces for the CMOS-based PRESENT-80 S-Box. The CPA attacks reveal the correct encryption key after 5120 power traces. Figure 6.14 shows the correlation coefficient starts appearing different after 40 power traces. The distinct power consumption, therefore, the current makes the CPA successful over the CMOS-based S-box of PRESENT-80 encryption.

The CCAL based S-box has better NED and NSD performance compared to CMOS. However, dual-rail adiabatic logic, e.g. 2-EE-SPFAL [9], and 2-SPGAL [10] have better NED and NSD values. It becomes important to see if CCAL based PRESENT-80 S-box is safe against the CPA attack. Similar to CMOS, we collected 12,000 power traces for the CCAL based PRESENT-80 S-box with 2N2P-PCG integrated into the design. Similar to our previous work on dual-rail adiabatic logic, 2-EE-SPFAL [9] and 2-SPGAL [10], the CCAL based S-box circuit protects the revelation of the encryption key. Therefore, higher NED and NSD value in CCAL compared to dual-rail logic does not affect the properties to protect the encryption key against the CPA attack.

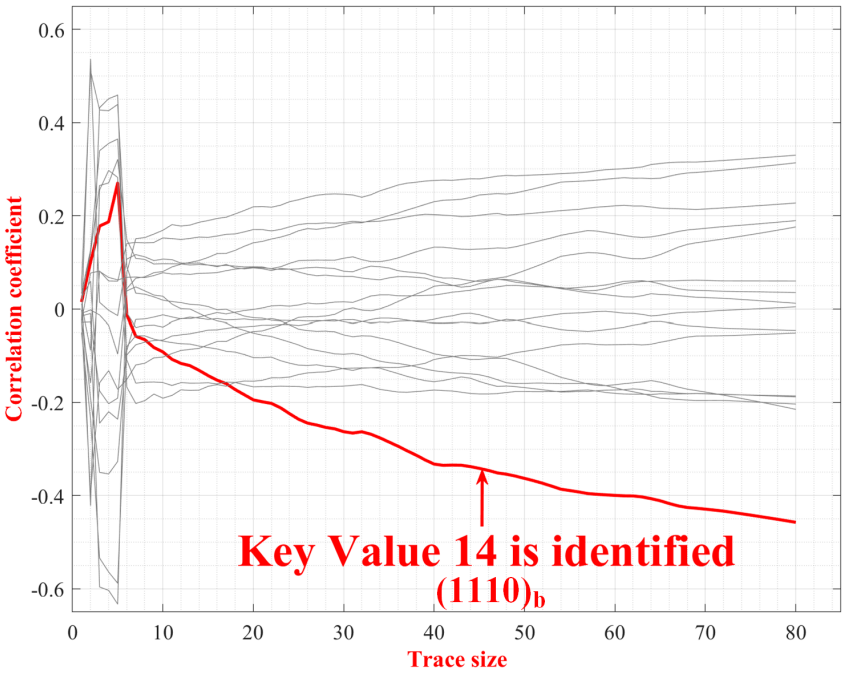

Figure 6.14: Successful Revelation of Key=14 in on one round of PRESENT-80 encryption designed with CMOS.

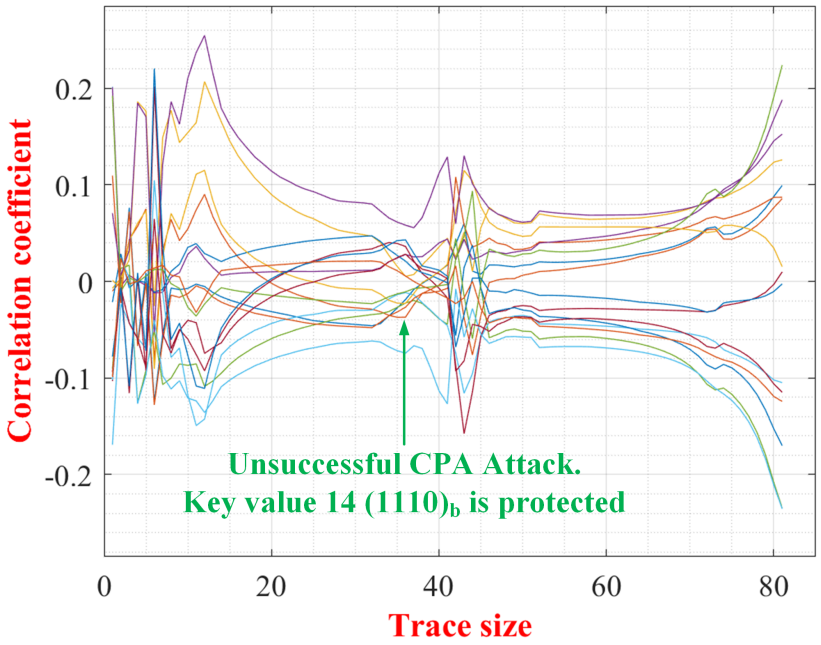

Figure 6.15: Unsuccessful CPA attack on one round of PRESENT-80 encryption designed with CCAL and 2N-PCG.

6.7 Summary

The cost and the reliability of the medical devices are the important factors to consider while selecting a technology with adiabatic logic. Bulk MOSFET at 45nm combined with adiabatic logic will provide a low-cost solution for medical devices that can also provide an energy-efficient and secure solution. Novel devices such as Junctionless MOSFET [172] [173]and Tunnel FET [174] [175] can also be explored with adiabatic logic for developing low-power and secure solutions. However, the designer should consider the cost and the reliability of the emerging devices when combined with adiabatic logic while making the design choice for medical devices. The low-frequency medical devices are vulnerable to side-channel attacks (e.g. Correlation Power Analysis (CPA) attack). The conventional approach to improve the CPA resistance results in an increase in power consumption. In this article, we used the single rail adiabatic circuit design technique called Clocked CMOS Adiabatic Logic (CCAL) to design cryptographic circuits in low-frequency medical devices. CCAL shows encouraging energy-saving and security performance compared to its dual-rail adiabatic logic and CMOS counterparts.

Further, the CCAL enables the designer to reduce the transistor count in cryptographic hardware compared to existing solutions based on adiabatic logic proposed in the literature. We also demonstrated the capability of the CCAL based logic to thwart the CPA attack and protect the encryption key. Therefore, CCAL can be a promising design choice for the designer of medical devices to increase their battery longevity with improved CPA resistance while keeping the transistor overhead to minimal. While designing single rail adiabatic logic circuits, the stability in the outputs should be considered while cascading the designs. The stable outputs can be produced by inserting the flip-flop to sample the correct output at each stage [176]. Another alternative approach to provide stable outputs could be to use noise reduction circuitry that can be added to restore the signal degraded [177]. Some possible future research direction would be to check the performance of the CCAL-based circuit implementation with different types of Power Clock Generator, e.g., switch capacitor, stepwise charging, etc.

Chapter 7

Conclusion and Future Directions

7.1 Conclusion

The burgeoning of smart computing devices and existing limitations security have resulted in a significant rise in attacks in recent years. The security framework developed should be readily adaptable to the existing infrastructure of smart computing devices. The objective of the research presented in this dissertation is to design hardware security primitives (TRNG and PUF) without incurring any additional hardware requirements. Secondly, to develop energy-efficient cryptographic circuit design techniques that are secure against Correlation Power Analysis (CPA) attack, a type of side-channel attack.

This dissertation highlights the importance of TRNG and PUF in generating the secure key, secure storage of the key, authentication, digital signature, nonce bit, salt bit, and padding bit generation in cryptographic operations. The existing TRNG and PUF come at the cost of additional transistor circuitry to be used as an entropy source, therefore, not suitable in space-savvy smart computing devices. The research in this dissertation report presents a novel way to explore the electrical response of the sensor as an entropy source. The proposed methodology has two primary advantages compared to existing TRNG and PUF. First, designing TRNG and PUF from existing sensor responses removes the need for additional dedicated hardware requirements and is beneficial in area-constrained miniaturized smart com-

puting devices. Secondly, the manufacturing process variation in each sensor is different, thus, tempering or replacing the sensor will result in a different response. Therefore, it enables to identify the physically compromised or malicious hardware replacement.

The key contribution from this dissertation report can be summarized as follow:

- The proposed TRNG and PUF prototypes are developed from existing photoresistor and photovoltaic solar cell sensors. As per the current statistic, 46% vulnerable IoT devices have at least one of the above sensors. Therefore, the proposed TRNG and PUF prototypes can be useful to improve existing security infrastructure.

- The proposed prototypes do not require additional interfacing hardware between sensors and computing units. Thus, they can be an option for space-limited smart computing devices. Further, the proposed prototypes can be easily posted over existing photoresistor and photovoltaic solar cell sensor-based devices as a software update.

- The lightweight scrambling method proposed in the TRNG prototype is suitable for limited computing devices, results in 32 times better random bit generation rate than existing prototypes. The proposed prototype has random bit entropy close to ideal value 1.

- We proposed a novel histogram-based technique to split the electrical response of the photovoltaic solar cell sensor electrical response. The proposed technique enables the integration of TRNG and PUF as one structure. The integrated TRNG-PUF architecture has approximately 34% better TRNG throughput and quality performance of TRNG and PUF response bits.

- To secure the cryptographic circuitry design inside the computing unit, we specifically worked on energy recovery computing (i.e., adiabatic circuit) that recovers the charge stored on load capacitor back to power-clocking circuitry rather than dissipating as heat in conventional CMOS logic.

- The proposed 2-SPGAL, the 2-phase sinusoidal clocking implementation of Symmetric Pass Gate Adiabatic Logic (SPGAL) shows better

energy efficiency and security performance for Lightweight Cryptography (LWC) cipher PRESENT compared to baseline CMOS.

- The 2-SPGAL shows improvement in security performance metrics, Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) compared to baseline CMOS logic used in conventional cryptographic circuit design. Further, we also show that, unlike its CMOS-based LWC cipher implementation, 2-SPGAL can withstand the CPA attack and protect the key revelation.

- Lastly, we explore Clocked CMOS Adiabatic Logic (CCAL) to design cryptographic circuitry. The CCAL based circuity is architecturally close to CMOS and requires approximately 45% fewer transistor counts compared to existing adiabatic logic-based implementation. Further, The CCAL based cryptographic circuits show further improvement in energy-saving compared to CMOS and its 2-phase adiabatic logic counterpart.

- Similar to the previously proposed 2-phase sinusoidal clocking counterpart (2-SPGAL), CCAL also thwarts the CPA attack and protects the key. Therefore, the CCAL can be a promising circuit design choice to implement cryptographic circuitry with better security performance with increased energy performance.

The research explored in this dissertation presents an important step to improve the security of both existing and future computing devices. The work presented in Chapter 3, 4 and 5 have been reviewed by scientific community. The research presented in Chapter 6 is currently under review for journal publication. The TRNG prototype and integrated TRNG-PUF prototype were designed using standard sensors and an ARM microcontroller. The adiabatic logic work was evaluated using CAD tools, Cadence Virtuoso. The simulation automation was realized in the Open Command Environment for Analysis (OCEAN) language and its use in the Cadence Virtuoso Design Environment. We can conclude that the proposed research in this dissertation can play a key role to improve the security in smart computing devices.

7.2 Future Work

In this dissertation, we explored the viability of designing the security primitives (e.g. TRNG and PUF) using the electrical response of the sensors. We also presented the circuit designing technique that results in improved energy efficiency and capability to withstand a CPA attack. However, the security concern of future embedded computing will be always a growing concern. As a result, the security approaches based on the hardware will attract significant interest in the future.

- We performed pre-layout schematic design, the simulation is performed by considering the ideal wires. In reality, wires occupy up to 40% of the area, thereby contributing a significant proportion to parasitic capacitance and resistance. The post-layout simulation to understand the effect of parasitic capacitance and resistance of micro-structures of the circuit. The evaluation of the circuit performance in post-layout gives higher confidence that the layout of the design will meet the desired specifications.

- Another interesting research direction is to design energy recovery-based TRNG-PUF using adiabatic logic. The adiabatic logic designed can be explored to design a low-power integrated TRNG-PUF design. The adiabatic logic operates on different phases and can result in more randomization. The performance of the PUF can be tested for power consumption analysis, uniformity, uniqueness, reliability, and bit-aliasing. The performance of the TRNG can be tested using NIST recommended Statistical Test Suite. Further, the energy consumption of the adiabatic TRNG-PUF can be compared with existing SRAM and magnetic memory-based integrated TRNG-PUF prototypes.

- The Integrated TRNG-PUF has less than 100% reliability performance for the PUF. For the critical security application, the security reliability needs to be improved. The work in [178], and [179] proposes the usage of Error-Correcting Codes (ECC) to improve the reliability. In the future direction, the ECC can be combined along with the PUF performance bit for improved reliability. Further, the performance of the TRNG-PUF can be tested for temperature and humidity variations.

- The existing TRNG-PUF is designed based on dividing the Gaussian probability distribution function into the static and dynamic parts.

The technique to divide the non-Gaussian response of the sensor into static and dynamic parts can be developed.

- After the silicon prototype of the adiabatic circuit-based prototype was developed, the interface of the sensor-based TRNG and PUF with the adiabatic cryptographic engine can be explored. In this problem, the TRNG, and PUF can generate the key, salt bits, initialization vector to be used in adiabatic logic-based cryptographic circuits. The secure data transfer between TRNG-PUF and adiabatic circuits needs to be established. The adiabatic PUF and sensor-based PUF can be used to mutually authenticate the sensor and the cryptographic engine. The successful completion of this problem will provide an alternate novel hardware security primitive platforms for IoT security.

Bibliography

[1] "Ics-cert year in review," Gartner Inc, MA, US. https://us-cert.cisa.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf, Last Accessed: 10-29-2021.

[2] J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 32–37, 2017.

[3] M. Fazion, "Vulnerabilities and security issues of iot devices," *Sikur Report*, no. 01022020, 2020.

[4] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the internet of things from the layered context," *Transactions on Emerging Telecommunications Technologies*, p. e3935, 2020.

[5] 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 *International workshop on cryptographic hardware and embedded systems*, pp. 450–466, Springer, 2007.

[6] S. D. Kumar, H. Thapliyal, A. Mohammad, and K. S. Perumalla, "Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware," *Integration*, vol. 58, pp. 369–377, 2017.

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

[8] S. K. Satpathy, S. K. Mathew, R. Kumar, V. Suresh, M. A. Anders, H. Kaul, A. Agarwal, S. Hsu, R. K. Krishnamurthy, and V. De, "An all-digital unified physically unclonable function and true random number generator featuring self-calibrating hierarchical von neumann extraction in 14-nm tri-gate cmos," *IEEE Journal of Solid-State Circuits*, vol. 54, no. 4, pp. 1074–1085, 2019.

[9] 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, 2020.

[10] 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, 2021.

[11] H. Li, Y. Zhang, and T. Yoshihara, "Clocked cmos adiabatic logic with low-power dissipation," in *2013 International SoC Design Conference (ISOCC)*, pp. 064–067, IEEE, 2013.

[12] G. Gardašević, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović, and M. Radonjić, "The iot architectural framework, design issues and application domains," *Wireless personal communications*, vol. 92, no. 1, pp. 127–148, 2017.

[13] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[14] "Cisco annual internet report (2018–2023) white paper," CISCO, CA, US, March 9, 2020. `https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf,` Last Accessed: 10-29-2021.

[15] K. M. Joe Berti and T. O'Hanlon, "Ibm iot," IBM, NY, US. `https://www.ibm.com/thought-leadership/institute-business-value/report/connected-operations%C2%A0#,` Last Accessed: 10-29-2021.

[16] K. L. Lueth, "State of the iot 2018: Number of iot devices now at 7b – market accelerating," IoT Analytics GmbH, Hamburg, Germany,

August 8, 2018. https://www.ibm.com/thought-leadership/institute-business-value/report/connected-operations%C2%A0#, Last Accessed: 10-29-2021.

[17] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *The internet of things*, pp. 389–395, Springer, 2010.

[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[19] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: Present and future challenges," *IEEE Internet of things journal*, vol. 5, no. 4, pp. 2483–2495, 2017.

[20] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[21] "Threat intelligence report 2020," Nokia, Espoo, Finland, 2020. https://onestore.nokia.com/asset/210088/, Last Accessed: 11-03-2021.

[22] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, "Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *arXiv preprint arXiv:2006.11929*, 2020.

[23] "Mid-year threat landscape report 2020," BitDefender, Bucharest, Romania, June, 2020. https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf, Last Accessed: 10-29-2021.

[24] K. Ashton *et al.*, "That 'internet of things' thing," *RFID journal*, vol. 22, no. 7, pp. 97–114, 2009.

[25] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:1501.02211*, 2015.

[26] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *2015 IEEE World Congress on Services*, pp. 21–28, IEEE, 2015.

[27] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, 2018.

[28] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber–physical systems and the internet-of-things," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 38–60, 2017.

[29] E. K. Wang, Y. Ye, X. Xu, S.-M. Yiu, L. C. K. Hui, and K.-P. Chow, "Security issues and challenges for cyber physical system," in *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, pp. 733–738, IEEE, 2010.

[30] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—a survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[31] D. Arney, K. K. Venkatasubramanian, O. Sokolsky, and I. Lee, "Biomedical devices and systems security," in *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 2376–2379, IEEE, 2011.

[32] T. Dimitriou and K. Ioannis, "Security issues in biomedical wireless sensor networks," in *2008 First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, pp. 1–5, IEEE, 2008.

[33] V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Minimum on-the-node data security for the next-generation miniaturized wireless biomedical devices," in *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1068–1071, IEEE, 2020.

[34] "2020 unit 42 iot threat report," Palo Alto Networks, CA, US, 2020. `https://start.paloaltonetworks.com/unit-42-iot-threat-report,` Last Accessed: 10-29-2021.

[35] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.

[36] 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.

[37] S. Moore, "Gartner predicts by 2025 cyber attackers will have weaponized operational technology environments to successfully harm or kill humans," Gartner Inc, MA, US, July 21, 2021. `https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we`, Last Accessed: 10-29-2021.

[38] "Alerts - national cyber awareness system," Cybersecurity and Infrastructure Security Agency, US. `https://us-cert.cisa.gov/ncas/alerts`, Last Accessed: 10-29-2021.

[39] G. Martin, P. Martin, C. Hankin, A. Darzi, and J. Kinross, "Cybersecurity and healthcare: how safe are we?," *Bmj*, vol. 358, 2017.

[40] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *IEEE 13th Int. Conf. on e-Health Networking, Applications and Services*, pp. 150–156, 2011.

[41] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform," *J. of Netw. and Computer Appl.*, vol. 107, pp. 1–21, 2018.

[42] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symp. on Security and Privacy (sp 2008)*, pp. 129–142, IEEE, 2008.

[43] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *Proc. of the ACM SIGCOMM 2011 Conf.*, pp. 2–13, 2011.

[44] M. Stipčević and Ç. K. Koç, "True random number generators," in *Open Problems in Mathematics and Computational Science*, pp. 275–315, Springer, 2014.

[45] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[46] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *International workshop on Cryptographic Hardware and Embedded Systems*, pp. 63–80, Springer, 2007.

[47] J.-L. Zhang, G. Qu, Y.-Q. Lv, and Q. Zhou, "A survey on silicon pufs and recent advances in ring oscillator pufs," *Journal of computer science and technology*, vol. 29, no. 4, pp. 664–678, 2014.

[48] G. Honan, N. Gekakis, M. Hassanalieragh, A. Nadeau, G. Sharma, and T. Soyata, "Energy harvesting and buffering for cyber physical systems: A review," *Cyber-Physical Systems: A Computational Perspective*, pp. 191–217, 2015.

[49] B. Haraoubia, *Nonlinear Electronics 1: Nonlinear Dipoles, Harmonic Oscillators and Switching Circuits*. Elsevier, 2018.

[50] "Pdv-p8104 datasheet," 2019.

[51] A. Degada and H. Thapliyal, "Harnessing uncertainty in photoresistor sensor for true random number generation in iot devices," in *2020 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–5, IEEE, 2020.

[52] A. Degada and H. Thapliyal, "An integrated trng-puf architecture based on photovoltaic solar cells," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 99–105, 2021.

[53] A. Degada and H. Thapliyal, "2-phase adiabatic logic for low-energy and cpa-resistant implantable medical devices," *IEEE Transactions on Consumer Electronics*, pp. 1–10, 2021.

[54] 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*, pp. 1–13, 2021.

[55] W. Stallings, L. Brown, M. D. Bauer, and A. K. Bhattacharjee, *Computer security: principles and practice*. Pearson Education Upper Saddle River, NJ, USA, 2012.

[56] J. Daemen and V. Rijmen, "Reijndael: The advanced encryption standard.," *Dr. Dobb's Journal: Software Tools for the Professional Programmer*, vol. 26, no. 3, pp. 137–139, 2001.

[57] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[58] K. McKay, L. Feldman, G. Witte, *et al.*, "Toward standardizing lightweight cryptography," tech. rep., National Institute of Standards and Technology, 2017.

[59] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the theory and application of cryptographic techniques*, pp. 417–426, Springer, 1985.

[60] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[61] P. Barreto, V. Rijmen, *et al.*, "The whirlpool hashing function," in *First open NESSIE Workshop, Leuven, Belgium*, vol. 13, p. 14, 2000.

[62] M. Rao, T. Newe, and I. Grout, "Secure hash algorithm-3 (sha-3) implementation on xilinx fpgas, suitable for iot applications," in *8th International Conference on Sensing Technology (ICST 2014), Liverpool John Moores University, Liverpool, United Kingdom, 2nd-4th September*, 2014.

[63] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "Nbc-maids: Naïve bayesian classification technique in multi-agent system-enriched ids for securing iot against ddos attacks," *The Journal of Supercomputing*, vol. 74, no. 10, pp. 5156–5170, 2018.

[64] M. A. Mughal, X. Luo, A. Ullah, S. Ullah, and Z. Mahmood, "A lightweight digital signature based security scheme for human-centered internet of things," *IEEE Access*, vol. 6, pp. 31630–31643, 2018.

[65] U. Chatterjee, V. Govindan, R. Sadhukhan, D. Mukhopadhyay, R. S. Chakraborty, D. Mahata, and M. M. Prabhu, "Building puf based authentication and key exchange protocol for iot without explicit crps in verifier database," *IEEE transactions on dependable and secure computing*, vol. 16, no. 3, pp. 424–437, 2018.

[66] Y. Zheng, X. Zhao, T. Sato, Y. Cao, and C.-H. Chang, "Ed-puf: Event-driven physical unclonable function for camera authentication in reactive monitoring system," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2824–2839, 2020.

[67] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (wbsn) based on physical unclonable function (puf)," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, pp. 1314–1318, IEEE, 2013.

[68] A. Braeken, "Puf based authentication protocol for iot," *Symmetry*, vol. 10, no. 8, 2018.

[69] J. Voris, N. Saxena, and T. Halevi, "Accelerometers and randomness: Perfect together," in *Proceedings of the Fourth ACM Conference on Wireless Network Security*, WiSec '11, (New York, NY, USA), pp. 115–126, ACM, 2011.

[70] S. L. Hong and C. Liu, "Sensor-based random number generator seeding," *IEEE Access*, vol. 3, pp. 562–568, 2015.

[71] G. Revadigar, C. Javali, W. Xu, A. V. Vasilakos, W. Hu, and S. Jha, "Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 2467–2482, Oct 2017.

[72] C. Erbay and S. Ergün, "Random number generator based on fuel cells," in *2018 New Generation of CAS (NGCAS)*, pp. 98–101, Nov 2018.

[73] C. Erbay and S. Ergïn, "Random number generator based on hydrogen gas sensor for security applications," in *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 709–712, Aug 2018.

[74] Y. Sun and B. Lo, "Random number generation using inertial measurement unit signals for on-body iot devices," 2018.

[75] C. Camara, P. Peris-Lopez, H. Martín, and M. Aldalaien, "Ecg-rng: A random number generator based on ecg signals and suitable for securing wireless sensor networks," *Sensors*, vol. 18, no. 9, 2018.

[76] C. Kösemen and G. Dalkiliç, "Designing a random number generator for secure communication with wisp," in *Proceedings of the International Conference on Compute and Data Analysis*, ICCDA '17, (New York, NY, USA), pp. 289–292, ACM, 2017.

[77] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, pp. 3–37, Springer, 2010.

[78] M. Feiri, J. Petit, and F. Kargl, "Efficient and secure storage of private keys for pseudonymous vehicular communication," in *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*, pp. 9–18, 2013.

[79] F. Syed, J. Nupur, A. Vichare, and A. Mishra, "Authentication of electronic control unit using arbiter physical unclonable functions in modern automobiles," in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, pp. 1–9, 2016.

[80] "Lightweight cryptography," National Institure of Standards and Technology (NIST), US. `https://csrc.nist.gov/Projects/lightweight-cryptography,` Last Accessed: 10-26-2021.

[81] P. Karl and M. Gruber, "A survey on the application of fault analysis on lightweight cryptography," in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–3, IEEE, 2021.

[82] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0475–0481, IEEE, 2019.

[83] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007.

[84] A. Chakraborti, T. Iwata, K. Minematsu, and M. Nandi, "Blockcipher-based authenticated encryption: how small can we go?," *Journal of Cryptology*, vol. 33, no. 3, pp. 703–741, 2020.

[85] J. Black and P. Rogaway, "A block-cipher mode of operation for parallelizable message authentication," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 384–397, Springer, 2002.

[86] P. H. Griffin, "Secure authentication on the internet of things," in *SoutheastCon 2017*, pp. 1–5, IEEE, 2017.

[87] C. Trinh, B. Huynh, J. Lansky, S. Mildeova, M. Safkhani, N. Bagheri, S. Kumari, and M. Hosseinzadeh, "A novel lightweight block cipher-based mutual authentication protocol for constrained environments," *IEEE Access*, vol. 8, pp. 165536–165550, 2020.

[88] D. Molnar, A. Soppera, and D. Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of rfid tags," in *International workshop on selected areas in cryptography*, pp. 276–290, Springer, 2005.

[89] A. Y. Poschmann, *Lightweight cryptography: cryptographic engineering for a pervasive world*. PhD thesis, Ruhr University Bochum, 2009.

[90] A. Luykx, B. Preneel, E. Tischhauser, and K. Yasuda, "A mac mode for lightweight block ciphers," in *International Conference on Fast Software Encryption*, pp. 43–59, Springer, 2016.

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

[92] J. A. Ambrose, R. G. Ragel, and S. Parameswaran, "Rijid: random code injection to mask power analysis based side channel attacks," in *Proc. of the 44th Annu. Design Automation Conf.*, pp. 489–492, 2007.

[93] D. May, H. L. Muller, and N. P. Smart, "Non-deterministic processors," in *Australasian Conf. on Information Security and Privacy*, pp. 115–129, Springer, 2001.

[94] D. May, H. Muller, and N. Smart, "Random register renaming to foil dpa," in *Int. Workshop on Cryptographic Hardware and Embedded Systems*, pp. 28–38, Springer, 2001.

[95] K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "A side-channel leakage free coprocessor ic in 0.18 μm cmos for embedded aes-based cryptographic and biometric processing," in *Proc. of the 42nd Annu. Design Automation conf.*, pp. 222–227, 2005.

[96] A. Moradi and A. Poschmann, "Lightweight cryptography and dpa countermeasures: A survey," in *Int. Conf. on Financial Cryptography and Data Security*, pp. 68–79, Springer, 2010.

[97] 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.

[98] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing.," *IACR Cryptol. ePrint Arch.*, vol. 2005, p. 388, 2005.

[99] 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.

[100] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in *International conference on the theory and applications of cryptographic techniques*, pp. 37–51, Springer, 1997.

[101] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *26th Int. Conf on VLSI design and 2013 12th Int. conf. on embedded systems*, pp. 203–208, IEEE, 2013.

[102] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *International workshop on cryptographic hardware and embedded systems*, pp. 16–29, Springer, 2004.

[103] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "Dpa-secured quasi-adiabatic logic (sqal) for low-power passive rfid tags employing s-boxes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 1, pp. 149–156, 2014.

[104] H. S. Raghav, V. A. Bartlett, and I. Kale, "Investigating the effectiveness of without charge-sharing quasi-adiabatic logic for energy efficient and secure cryptographic implementations," *Microelectronics J.*, vol. 76, pp. 8–21, 2018.

[105] H. S. Raghav and I. Kale, "A balanced power analysis attack resilient adiabatic logic using single charge sharing transistor," *Integr. the VLSI J.*, vol. 69, pp. 147–160, 2019.

[106] C. Monteiro, Y. Takahashi, and T. Sekine, "Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks," in *36th IEEE Int. Conf. on Telecommunications and Signal Processing (TSP)*, pp. 732–736, 2013.

[107] B. Fadaeinia and A. Moradi, "3-phase adiabatic logic and its sound sca evaluation," *IEEE Trans. on Emerging Topics in Computing*, 2020.

[108] B. Halak, M. Zwolinski, and M. S. Mispan, "Overview of puf-based hardware security solutions for the internet of things," in *2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1–4, IEEE, 2016.

[109] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of puf-based" unclonable" rfid ics for anti-counterfeiting and security applications," in *2008 IEEE international conference on RFID*, pp. 58–64, IEEE, 2008.

[110] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., Booz-Allen and Hamilton Inc Mclean Va, 2001.

[111] E. Barker and L. Bassham, "Random bit generation - guide to the statistical tests," National Institute of Standards and Technology (NIST), MD, US, May 24, 2016. `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf`, Last Accessed: 10-29-2021.

[112] H. Krawczyk, "Cryptographic extraction and key derivation: The hkdf scheme," in *Annual Cryptology Conference*, pp. 631–648, Springer, 2010.

[113] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in iot systems using physical unclonable functions," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327–1340, 2017.

[114] M. Barbareschi, P. Bagnasco, and A. Mazzeo, "Authenticating iot devices with physically unclonable functions models," in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pp. 563–567, IEEE, 2015.

[115] E. Öztürk, G. Hammouri, and B. Sunar, "Towards robust low cost authentication for pervasive devices," in *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pp. 170–178, IEEE, 2008.

[116] S. Katzenbeisser, Ü. Kocabaş, V. Van Der Leest, A.-R. Sadeghi, G.-J. Schrijen, and C. Wachsmann, "Recyclable pufs: Logically reconfigurable pufs," *Journal of Cryptographic Engineering*, vol. 1, no. 3, p. 177, 2011.

[117] M. Majzoobi, M. Rostami, F. Koushanfar, D. S. Wallach, and S. Devadas, "Slender puf protocol: A lightweight, robust, and secure authentication by substring matching," in *2012 IEEE Symposium on Security and Privacy Workshops*, pp. 33–44, IEEE, 2012.

[118] W. Che, M. Martin, G. Pocklassery, V. K. Kajuluri, F. Saqib, and J. Plusquellic, "A privacy-preserving, mutual puf-based authentication protocol," *Cryptography*, vol. 1, no. 1, p. 3, 2017.

[119] M. van Dijk and U. Rührmair, "Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results.," *IACR Cryptol. EPrint Arch.*, vol. 2012, p. 228, 2012.

[120] J. Kong, F. Koushanfar, P. K. Pendyala, A.-R. Sadeghi, and C. Wachsmann, "Pufatt: Embedded platform attestation based on novel processor-based pufs," in *2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, pp. 1–6, IEEE, 2014.

[121] S. Schulz, A. Schaller, F. Kohnhäuser, and S. Katzenbeisser, "Boot attestation: Secure remote reporting with off-the-shelf iot sensors," in *European Symposium on Research in Computer Security*, pp. 437–455, Springer, 2017.

[122] Y. Lao, B. Yuan, C. H. Kim, and K. K. Parhi, "Reliable puf-based local authentication with self-correction," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 2, pp. 201–213, 2016.

[123] A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, and M. Yung, "End-to-end design of a puf-based privacy preserving authentication protocol," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 556–576, Springer, 2015.

[124] A. R. Elaine Barker and R. Davis, "Recommendation for cryptographic key generation," National Institute of Standards and Technology (NIST), MD, US, June 2020. `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf`, Last Accessed: 10-29-2021.

[125] T. Kowsalya, R. G. Babu, B. Parameshachari, A. Nayyar, and R. M. Mehmood, "Low area present cryptography in fpga using trng-prng key generation," *CMC-COMPUTERS MATERIALS & CONTINUA*, vol. 68, no. 2, pp. 1447–1465, 2021.

[126] A. R. A. V. Elaine Barker, Lily Chen and R. Davis, "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography," National Institute of Standards and Technology (NIST), MD, US, APR 2018. `https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf`, Last Accessed: 10-29-2021.

[127] L. C. Elaine Barker and R. Davis, "Recommendation for key-derivation methods in key-establishment schemes," National Institute of Standards and Technology (NIST), MD, US, Aug 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf, Last Accessed: 10-29-2021.

[128] H. Thapliyal, "Internet of things-based consumer electronics: Reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms," *IEEE Consumer Electronics Magazine*, vol. 7, pp. 66–67, Jan 2018.

[129] I. J. Gedeon, P. Snively, C. Frey, W. Almuhtadi, and S. P. Mohanty, "Privacy and security by design," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 76–77, 2020.

[130] S. P. Mohanty, "Security and privacy by design is key in the internet of everything (ioe) era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, 2020.

[131] M. Varchola, M. Drutarovsky, and V. Fischer, "New universal element with integrated puf and trng capability," in *2013 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, pp. 1–6, 2013.

[132] S. Larimian, M. R. Mahmoodi, and D. B. Strukov, "Lightweight integrated design of puf and trng security primitives based on eflash memory in 55-nm cmos," *IEEE Transactions on Electron Devices*, vol. 67, no. 4, pp. 1586–1592, 2020.

[133] V. Rožić, B. Yang, W. Dehaene, and I. Verbauwhede, "Iterating von neumann's post-processing under hardware constraints," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 37–42, IEEE, 2016.

[134] C. Labrado and H. Thapliyal, "Design of a piezoelectric-based physically unclonable function for iot security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2770–2777, 2019.

[135] "Obesity and overweight," World Health Organization. https://www.who.int/news-room/fact-sheets/detail/obesity-and-overweight, Last Accessed: 10-2-2021.

[136] "Chronic disease in america," Center for Disease Control (CDC). https://www.cdc.gov/chronicdisease/tools/infographics.htm, Last Accessed: 10-2-2021.

[137] T. G. Mahn, "Wireless medical technologies: Navigating government regulation in the new medical age," *Fishs Regulatory & Government Affairs Group*, 2013.

[138] "Short Range Devices (SRD); Ultra Low Power Active Medical Implants (ULP-AMI) and accessories (ULP-AMI-P) operating in the frequency range 9 kHz to 315 kHz Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU ," standard, ETSI (European Telecommunications Standards Institute), Sophia-Antipolis, France, June 2016.

[139] S. Hanna, "Regulations and standards for wireless medical applications," in *Proceedings of the 3rd international symposium on medical information and communication technology*, pp. 23–26, Citeseer, 2009.

[140] E. Völgyi, F. A. Tylavsky, A. Lyytikäinen, H. Suominen, M. Alén, and S. Cheng, "Assessing body composition with dxa and bioimpedance: effects of obesity, physical activity, and age," *Obesity*, vol. 16, no. 3, pp. 700–705, 2008.

[141] S. B. Rutkove, K. S. Lee, C. A. Shiffman, and R. Aaron, "Test–retest reproducibility of 50 khz linear-electrical impedance myography," *Clinical Neurophysiology*, vol. 117, no. 6, pp. 1244–1248, 2006.

[142] H. Wi, H. Sohal, A. L. McEwan, E. J. Woo, and T. I. Oh, "Multi-frequency electrical impedance tomography system with automatic self-calibration for long-term monitoring," *IEEE transactions on biomedical circuits and systems*, vol. 8, no. 1, pp. 119–128, 2013.

[143] Y. Yang and J. Jia, "A multi-frequency electrical impedance tomography system for real-time 2d and 3d imaging," *Review of Scientific Instruments*, vol. 88, no. 8, p. 085110, 2017.

[144] "Eit pioneer set," Swisstom AG, Switzerland. http://www.swisstom.com/wp-content/uploads/Swisstom_brochure-PioneerSet_GB_1ST500-102_Rev002_web.pdf, Last Accessed: 10-1-2021.

[145] A. Hedayatipour, S. Aslanzadeh, S. H. Hesari, M. A. Haque, and N. McFarlane, "A wearable cmos impedance to frequency sensing system for non-invasive impedance measurements," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 14, no. 5, pp. 1108–1121, 2020.

[146] L. Gerlach, G. Payá-Vayá, and H. Blume, "A survey on application specific processor architectures for digital hearing aids," *Journal of Signal Processing Systems*, pp. 1–16, 2021.

[147] C. Kuhlmann, A. P. Khandhar, R. M. Ferguson, S. Kemp, T. Wawrzik, M. Schilling, K. M. Krishnan, and F. Ludwig, "Drive-field frequency dependent mpi performance of single-core magnetite nanoparticle tracers," *IEEE transactions on magnetics*, vol. 51, no. 2, pp. 1–4, 2015.

[148] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1174–1188, 2014.

[149] M. Zhang, A. Raghunathan, and J. K, "Towards trustworthy medical devices and body area networks," in *Proceedings of the 50th Annual Design Automation Conference*, pp. 1–6, 2013.

[150] "Medical applications user guide," NXP Semiconductors. `https://www.nxp.com/docs/en/user-guide/MDAPPUSGDRM118.pdf`, Last Accessed: 10-1-2021.

[151] L. Bu and M. G. Karpovsky, "A design of secure and reliablewireless transmission channel for implantable medical devices.," in *ICISSP*, pp. 233–242, 2017.

[152] L. Bu, M. G. Karpovsky, and M. A. Kinsy, "Bulwark: Securing implantable medical devices communication channels," *Computers & Security*, vol. 86, pp. 498–511, 2019.

[153] G. Hunt, G. Letey, and E. Nightingale, "The seven properties of highly secure devices," *tech. report MSR-TR-2017-16*, 2017.

[154] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *2010 IEEE global telecommunications conference GLOBECOM 2010*, pp. 1–5, IEEE, 2010.

[155] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Transactions on Biomedical circuits and Systems*, vol. 7, no. 6, pp. 871–881, 2013.

[156] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 30–39, 2008.

[157] S. Hosseini-Khayat, "A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices," in *205th Int. Symp. on Medical Information and Communication Technology*, pp. 6–9, 2011.

[158] J. Fan, O. Reparaz, V. Rožić, and I. Verbauwhede, "Low-energy encryption for medical devices: Security adds an extra design dimension," DAC '13, (New York, NY, USA), Assoc. for Comput. Machinery, 2013.

[159] M. M. Kermani, M. Zhang, A. Raghunathan, and N. K. Jha, "Emerging frontiers in embedded security," in *26th Int. Conf. on VLSI Design and 12th Int. Con. on Embedded Systems*, pp. 203–208, 2013.

[160] S. Maji, U. Banerjee, S. H. Fuller, M. R. Abdelhamid, P. M. Nadeau, R. T. Yazicigil, and A. P. Chandrakasan, "A low-power dual-factor authentication unit for secure implantable devices," in *IEEE Custom Integrated Circuits Conf. (CICC)*, pp. 1–4, 2020.

[161] S. Yin, M. Kim, D. Kadetotad, Y. Liu, C. Bae, S. J. Kim, Y. Cao, and J.-S. Seo, "A 1.06- μ w smart ecg processor in 65-nm cmos for real-time biometric authentication and personal cardiac monitoring," *IEEE J. Solid-State Circuits*, vol. 54, no. 8, pp. 2316–2326, 2019.

[162] A. G. Dickinson and J. S. Denker, "Adiabatic dynamic logic," *IEEE J. Solid-State Circuits*, vol. 30, no. 3, pp. 311–315, 1995.

[163] J. Lim, D.-G. Kim, and S.-I. Chae, "A 16-bit carry-lookahead adder using reversible energy recovery logic for ultra-low-energy systems," *IEEE J. Solid-State Circuits*, vol. 34, no. 6, pp. 898–903, 1999.

[164] S. G. Younis and T. F. Knight, "Non-dissipative rail drivers for adiabatic circuits," in *Proc. of Sixteenth IEEE Conf. on Advanced Research in VLSI*, pp. 404–414, 1995.

[165] S. Maheshwari and I. Kale, "Impact of adiabatic logic families on the power-clock generator energy efficiency," in *15th Conf. on Ph.D Research in Microelectronics and Electronics (PRIME)*, pp. 25–28, 2019.

[166] M. J. Dworkin, *Sp 800-38A. Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. National Institute of Standards & Technology, 2001. [Online; accessed 05-May-2021].

[167] Y. Takahashi, T. Sekine, and M. Yokoyama, "Two-phase clocked cmos adiabatic logic," *Far East J. Electronics and Communications*, vol. 3, no. 1, pp. 17–34, 2009.

[168] 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.

[169] T. N. Theis and P. M. Solomon, "In quest of the "next switch": prospects for greatly reduced power dissipation in a successor to the silicon field-effect transistor," *Proceedings of the IEEE*, vol. 98, no. 12, pp. 2005–2014, 2010.

[170] T. N. Theis and H.-S. P. Wong, "The end of moore's law: A new beginning for information technology," *Computing in Science & Engineering*, vol. 19, no. 2, pp. 41–50, 2017.

[171] Y. Zhang, *Research on Low Power Technology by AC Power Supply Circuits*. PhD thesis, Waseda University, Tokyo, Japan, 2012.

[172] S. Roy, G. Jana, and M. Chanda, "Analysis of sub-threshold adiabatic logic model using junctionless mosfet for low power application," *Silicon*, pp. 1–9, 2021.

[173] S. D. Kumar, H. Thapliyal, and A. Mohammad, "Finsal: Finfet-based secure adiabatic logic for energy-efficient and dpa resistant iot devices," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 110–122, 2017.

[174] J.-S. Liu, M. B. Clavel, and M. K. Hudait, "Tbal: Tunnel fet-based adiabatic logic for energy-efficient, ultra-low voltage iot applications," *IEEE Journal of the Electron Devices Society*, vol. 7, pp. 210–218, 2019.

[175] H. Thapliyal, T. Varun, and S. D. Kumar, "Low-power and secure lightweight cryptography via tfet-based energy recovery circuits," in *2017 IEEE International Conference on Rebooting Computing (ICRC)*, pp. 1–4, IEEE, 2017.

[176] C. Rolfes, A. Poschmann, G. Leander, and C. Paar, "Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents," in *International Conference on Smart Card Research and Advanced Applications*, pp. 89–103, Springer, 2008.

[177] Y. Ye and K. Roy, "Qserl: Quasi-static energy recovery logic," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 2, pp. 239–248, 2001.

[178] B. Colombier, L. Bossuet, V. Fischer, and D. Hély, "Key reconciliation protocols for error correction of silicon puf responses," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1988–2002, 2017.

[179] Y. Wen and Y. Lao, "Efficient puf error correction through response weighting," in *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 849–852, IEEE, 2018.

Vita

Amitkumar Dalpatray Degada

Education

Sardar Vallabhbhai National Institute of Technology, Surat, India
Masters of Technology in Electronics - Communication Systems, July 2009

Bhavnagar University, Bhavnagar, India
Bachelors of Engineering, Electronics and Communication, July 2006

Awards

1. Received "Best Paper Award - Second Place" at 39th IEEE International Conference on Consumer Electronics (ICCE 2021), 2021, for our paper titled, "2-SPGAL: 2-Phase Symmetric Pass Gate Adiabatic Logic for Energy-Efficient Secure Consumer IoT".

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. A. Degada and H. Thapliyal, "Single-Rail Adiabatic Logic for Energy-Efficient and CPA-Resistant Cryptographic Circuit in Low-Frequency Medical Devices" in IEEE Open Journal of Nanotechnology, pp. 1-13, Submitted on: October 2021. **(Under Review)**
2. A. Degada and H. Thapliyal, "2-Phase Adiabatic Logic For Low-Energy and CPA-Resistant Implantable Medical Devices." in IEEE Transactions on Consumer Electronics, pp. 1-10, Submitted on: June 2021. **(Under Review)**

3. A. Degada and H. Thapliyal, "An Integrated TRNG-PUF Architecture Based on Photovoltaic Solar Cells," in IEEE Consumer Electronics Magazine, vol. 10, no. 4, pp. 99-105, 1 July 2021

4. A. Degada, H. Thapliyal and S. P. Mohanty, "Smart Village: An IoT Based Digital Transformation." 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), 2021, pp. 1-5.

5. A. Degada and H. Thapliyal, "2-SPGAL: 2-Phase Symmetric Pass Gate Adiabatic Logic for Energy-Efficient Secure Consumer IoT," 2021 IEEE International Conference on Consumer Electronics (ICCE), 2021, pp. 1-6.

6. A. Degada and H. Thapliyal, "Harnessing Uncertainty in Photoresistor Sensor for True Random Number Generation in IoT Devices," 2020 IEEE International Conference on Consumer Electronics (ICCE), 2020, pp. 1-5.