5-1-2023

A CURRENT TO DIGITAL CONVERTER FOR POWER SIGNATURE GENERATION APPLICATIONS

ARUNIMA AINDRILA BADHON
Southern Illinois University Carbondale, arunima.ece2k13@gmail.com

A CURRENT TO DIGITAL CONVERTER FOR POWER SIGNATURE GENERATION APPLICATIONS

by

Arunima Aindrila Badhon

B.S., Khulna University of Engineering and Technology, 2018

A Thesis
Submitted in Partial Fulfillment of the Requirements for the
Master of Science Degree

School of Electrical, Computer and Biomedical Engineering
in the Graduate School
Southern Illinois University Carbondale
May 2023

THESIS APPROVAL

A CURRENT TO DIGITAL CONVERTER FOR POWER SIGNATURE GENERATION APPLICATIONS

by

Arunima Aindrila Badhon

A Thesis Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Electrical & Computer Engineering

Approved by:

Dr. Haibo Wang, Chair

Dr. Chao Lu

Dr. Ying Chen

Graduate School
Southern Illinois University Carbondale
October 26, 2022

AN ABSTRACT OF THE THESIS OF

Arunima Aindrila Badhon, for the Master of Science degree in Electrical & Computer Engineering, presented on October 26, 2022, at Southern Illinois University Carbondale.

TITLE: A CURRENT TO DIGITAL CONVERTER FOR POWER SIGNATURE GENERATION APPLICATIONS

MAJOR PROFESSOR: Dr. Haibo Wang

The security of IoT devices is significantly increasing as a consequence of the widespread usage of the Internet of Things (IoT) in applications that include confidential data and implementation of important control decisions using those data. Because of their cheap cost and computational limitations, IoT devices confront significant obstacles in safeguarding. Among the variety of devised tactics analyzing power is one of the most potential strategies to address such challenges. However, due to the size, cost, and power consumption of power analysis devices, this strategy is not suited for many IoT applications. In this thesis, two techniques for collecting power signatures were proposed. A commercial 130nm CMOS technology is used to construct two circuits for each technique. For the purpose of determining how correctly the setups function, a considerable number of simulations are run under various conditions, and the results are assessed.

ACKNOWLEDGMENTS

I would like to express my gratitude to Dr. Haibo Wang for helping me to finish my thesis work and for giving me advice along the way. His ongoing oversight made it possible to have a thorough grasp of the research field. Also, I would like to thank Dr. Chao Lu and Dr. Ying Chen for serving as members of my thesis approval committee. Ashish Mahanta has also earned my sincere gratitude for his assistance throughout the earlier stages of this endeavor. In closing, I would like to express my gratitude to the College of Engineering for its consistent cooperation during my whole years of study at Southern Illinois University, Carbondale.

DEDICATION

This work is dedicated to my family, who supported me in every way while I adapted to a new environment overseas and encouraged me to seek higher education.

TABLE OF CONTENTS

CHAPTER PAGE

ABSTRACT i

ACKNOWLEDGMENTS ii

DEDICATION iii

LIST OF TABLES v

LIST OF FIGURES vi

CHAPTERS

CHAPTER 1 – Introduction 1

CHAPTER 2 – Related Work 4

CHAPTER 3 – Proposed Current to Digital Conversion Techniques 9

CHAPTER 4 – Circuit Implementation and Simulation Results 19

CHAPTER 5 – Conclusion and Future Work 39

REFERENCES 40

VITA 44

LIST OF TABLES

TABLE PAGE

Table 1 - Comparison Between Current Sources Being Monitored and the Calculated Current Values Found from Different Setups for the 1st Method 36

Table 2 - Comparison Between Current Sources Being Monitored and the Calculated Current Values Found from Different Setups for the 2nd Method 37

Table 3 - Statistics of Error for 1st Method 38

Table 4 - Statistics of Error for 2nd Method 38

LIST OF FIGURES

FIGURE PAGE

Figure 1.1 - Setup for Existing Methods to Capture Power Trace.……………….……………6

Figure 3.1 - Block Diagram of the First Proposed Method…………………….…………..10

Figure 3.2 - Operation of the 1st Proposed Method ……………………………………...11

Figure 3.3 - Block Diagram of the Second Proposed Method………………….………..13

Figure 3.4 - Operation of the 2nd Proposed Method ……………………………………14

Figure 3.5 - Output Error at Different Input Current Levels Considering Excess Charge in Capacitor 16

Figure 3.6 - Output Error at Different Input Current Levels Considering Excess Charge in Capacitor and Offset Voltage of Comparator 18

Figure 4.1 - The Comparator Circuit……………………………………………….20

Figure 4.2 - MOSFET Circuit Used in Comparator……………………………..21

Figure 4.3- Simulation Result of the Comparator……………………………......22

Figure 4.4 - Circuit Implementation for 1st Proposed Method with Comparator ……………....23

Figure 4.5 - Simulation of the Circuit for 1st Method with Comparator ($I_{ref} > I_{in}$)…….........24

Figure 4.6 - Relative Error vs Input Current Curve for 1st Method Implemented with Comparator 25

Figure 4.7 - Circuit Implementation for 2nd Proposed Method with Comparator ……………...27

Figure 4.8 - Simulation of the Circuit for 2nd Method with Comparator ……….…………….…28

Figure 4.9 - Relative Error vs Input Current Curve for 2nd Method Implemented with Comparator 29

Figure 4.10 - Zoomed in DC Sweep simulated Voltage Transfer Curve………...……………30

Figure 4.11 - Circuit Implementation for 1st Proposed Method with Inverter…... …………......31

Figure 4.12 - Simulation of the Circuit for 1st Method with Inverter $(I_{ref} > I_{in})$……………......32

Figure 4.13 - Relative Error vs Input Current Curve for 1st Method Implemented with Inverter 32

Figure 4.14 - Circuit Implementation for 2nd Proposed Method with Inverter…....………….......33

Figure 4.15 - Simulation of the Circuit for 2nd Method with Inverter…………………..........34

Figure 4.16 - Relative Error vs Input Current Curve for 2nd Method Implemented with Inverter 35

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION AND OBJECTIVES

Internet of Things (IoT) is a revolutionary technology that has been quietly advancing over the past few years and is now influencing our future. Nowadays, IoT devices have been used worldwide in a variety of applications, such as healthcare, smart cities, smart grid system, cognitive warehouses, connected logistics, self-driven cars, supply chain system, earthquake detection, a smart farming, home automation, human protection, etc. They contribute to making a comfortable and connected lifestyle with the purpose of minimizing labor and eradicating the possibility of human mistakes. Often, IoT devices are used in collecting, storing, and transmitting confidential and sensitive data including personally identifiable information. Such devices are also used to implement important control decisions with the help of collected data.

Even with all these advantages, there are still some hazards. One of the biggest issues with the Internet of Things is privacy and security [1, 2]. Any vulnerability or poorly protected IoT devices can lead to a hacker attack or a catastrophic failure, affecting millions of people and causing catastrophic consequences to society. In this way IoT system has inevitably become an enticing playground for cybercriminals. Most of the technological potential problems are comparable to those encountered with traditional data centers, workstations, and cellphones. These vulnerabilities include employing weak authorization, failure to change default credentials, sending unencrypted messages between endpoints, Command injection, Man-in-the-middle exploits, and failing to implement security upgrades properly [3].

There are extra difficulties in ensuring the security of IoT systems because no attempt has been successful in maximizing our present security capabilities, which were developed with traditional IT equipment and assets. These existing security techniques are incompatible with IoT devices due to a number of reasons [4]. First, many IoT devices are unable to perform robust, resource-intensive security activities due to significant operational constraints on the processing capacity available to them. Because computational capacity for encryption is limited, it is difficult to apply computationally intensive efficient built-in security measures given that they necessitate a considerable amount of power and expenditures. Because of the inadequate computer processing power of most IoT devices, they may nevertheless be corrupted by malware, which is frequently practiced by hackers since it is both versatile and financially viable. Furthermore, it will be difficult for device manufacturers to apply a single security standard because to the large variety of IoT devices, which range from modest microcontroller-based sensors to powerful server-class processors. These complex architectures of hardware and numerous software systems established in IoTs render it more difficult to improve global security techniques and to conduct software upgrades.

Recent studies indicate that monitoring power signature is a promising approach to enhance IoT security [5, 6, 7]. However, the existing methods to capture device power signatures are shortcoming while they are used in small scale devices. Therefore, these strategies have not been deployed successfully in the field of improve the security of tiny IoT devices [21, 22, 23]. Due to the requirement of heavy and massive equipment such as oscilloscope, spectrum analyzers, etc. which are also expensive to obtain the power trace or extract the power signature these methods are unsuitable for IoT devices.

In [21, 22], an integrated power signature generation circuit is presented. However, that circuit requires large off-chip capacitance resulting in a large footprint on the circuit board which is not desired. Motivated by this observation, this research intends to develop a power signature generation circuit that directly converts sampled current to digital value without using large off-chip capacitance.

1.2 CONTRIBUTION OF THE RESEARCH WORK

In this work, we present two methods for capturing IoT power signature without using large off-chip capacitors. The first method generates digital data that are proportional to the analog current values with high linearity. However, it requires a large current reference value. The second method relaxes this requirement but sacrifices the linearity between the generated digital data and analog current value. It also incurs large inaccuracy when the input current value is large.

Such inaccuracies are examined in this work. The circuit is designed and simulated with both ideal components and constructed components. A commercial CMOS 130 nanometer technology has been used to construct and simulate the suggested circuit. The simulation outcomes demonstrate the proposed circuit's exceptional measurement precision.

1.3 THESIS ORGANIZATION

Following is how the rest of this thesis is structured: Various existing methods of IoT security and power signature generating circuits are briefly discussed in Chapter 2 of this book. Two different methods are proposed in Chapter 3 to collect power signature generation along with the mathematical derivation. The constructed circuit for measuring current in the range of microamperes is described and simulation results for various settings are shown in Chapter 4 to support the operation of the circuit. The thesis is concluded in Chapter 5 along with a discussion of possible future study topics.

CHAPTER 2

RELATED WORK

There are significant research efforts being carried out to develop various techniques to boost IoT security. Light-weight encryption technique [9, 10, 11, 12, 13, 14], physically unclonable functions (PUFs) [15, 16, 17, 18, 19], antitampering sensors [20] and so on are usually used to counter the rising threat of cyberattacks stemming from insecure Internet of Things (IoT) devices [21, 22, 23, 24]. The implementation of lightweight encryptions may be done with hardware or software and requires less processing power and memory. But they frequently experience the negative effects of lengthy encryption times and the consistent usage of the same key across all encryption operations. On the other hand, although PUFs have distinctive identifying features due to physical variances that naturally produce during production that can be employed to generate encryption keys or identify individual devices, recently emerging machine learning-based attack techniques offer extreme challenges for PUFs [18, 19]. In antitampering method an integrated module is used which employs encryption and an encapsulating packaging barrier that is responsive to a minimum one physical characteristic of the encapsulation in order to perform the encryption and/or decryption by extracting the key therefrom, preventing access to the circuit by tampering with the encapsulation. However, it would be unacceptable if the outcome of a change in the encapsulation parameter was an unmodified key principle [20].

In the meantime, recent studies on the Security and Privacy Problems of IoTs show that side channel attacks based on power analysis are successfully obtaining encryption keys and confidential information [25, 26, 27, 28, 29]. These side This attack takes advantage of the close connection between circuit functionality and power consumption. An attacker can infer activity of a system by monitoring, gathering, and then analyzing data about the power utilized by that system or one of its subsystems [30]. Monitoring power consumption, or its more abstract representations like power signatures or power fingerprinting, can be a powerful method for identifying abnormality in the operation of compromised devices or systems because abnormal power usage is a solid sign that a device or system has been manipulated due to a detrimental attack [21, 22, 23]. In the PFP monitoring technique, a physical sensor is used to capture fine-grained power consumption indications such as power traces or fingerprints that develop during the changes between one command and another. It is possible to tell if a malicious attack has been successfully deployed during an operation if a departure from the expected behavior is detected while comparing the observed traces with reliable references [31]. This method has been widely used to: check the integrity of software defined radio of large electronic system [32], detect the execution of malware [33], and uniquely identify high performance computers [34]. Admittedly, the existing techniques to capture the power traces typically require bulky machineries, such as oscilloscopes or data acquisition instruments, which are power hungry. For this why, PFP method is not used to enhance the security of miniature IoT devices [21, 22, 23].

2.1 EXISTING POWER MEASUREMENT METHODS FOR POWER ANALYSIS

The accuracy of the data and the accessibility of measuring tools are the key concerns of the existing current power trace methodologies. One of these techniques was utilized in certain publications where a tiny resistor was connected in series with the path of the device's power source or ground [32, 35, 36]. Then, a data collection device or oscilloscope with data capturing capacity is used to obtain the voltage drop across the series resistor, as shown in Figure 1.1(a). The recorded voltage is divided by the value of the added resistance to calculate the current consumption. In this approach we can only retrieve the current consumption data. Adding voltage and current sensors to a PCB board and installing it at the power supply channel as figure

1.1 (b) [33] is another typical method. Although we can get both current and voltage data in this way, and the data is highly reliable because it comes from an analog sensor, we will need extra equipment to transform the data into a digital value. These instruments are large and power-hungry, making them inappropriate for use with tiny IoT.

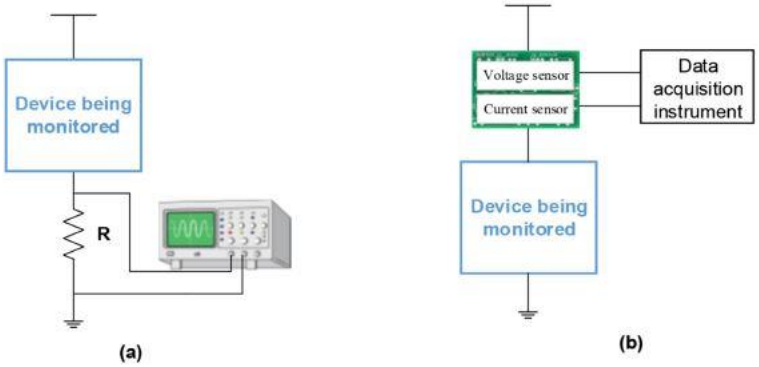

Figure 1.1 Setup for Existing Methods to Capture Power Trace

Dedicated power monitoring circuitry with current detecting resistors is integrated into some sensors. These sensors are also set up in the power supply path. Operational amplifier circuits are used to measure the voltage of these resistors, and the voltage is then transformed to a digital value by ADCs or microcontrollers. Despite their modest footprints, such designs are sensitive to adversarial cyber-attacks because of the employment of additional components and the exposure of PCB lines. All these systems entail adding sensing components into the power supply line, which has a voltage drop resulting in undesirable wastage of energy, and other factors in some applications [21].

One of the current sensors based on Faraday's law of induction is the Rogowski Coil. Although with this method we can measure direct currents as the basic principle is calculated with the detection of a flux change, which is proportional to a current change we must know the current at the beginning of the process. The real integrators may employ small input offset voltage and can have a significant gain at low frequency. Hence, practical Rogowski coils are not suitable to measure low-frequency currents. Magnetic field-based sensors such as open loop and closed loop technology, Hall Effect sensor are attractive methods too. Open loop technology has hysteresis and eddy current losses, and can lead to excessive heating. Though the closed loop technology doesn’t have these current losses the disadvantages of this method is the complicated construction, larger cost, and increased bulk. Numerous kinds of Hall Effect sensors for current sensing are available which are appropriate for sensing huge currents. But these sensors are incapable to sense small amount of current because of the weak magnetic field produced by small currents. A slotted toroid can be used to concentrate the generated flux field to improve the sensitivity. But this is not suitable as it increases the expense and complexity of the current detecting circuit. [21, 27].

2.2 AVAILABLE BUILT-IN CURRENT SENSORS

Currently available built-in current sensors analyze integrated circuit (IC) current consumption. These are designed for IDDQ and IDDT assessment [37, 38], or hardware Trojan diagnosis [39, 40]. These circuits use power gating devices as current sensing resistors and convert the drain to source voltage of those devices to a current by using current mirror type circuits. But they can only identify the current value during a specific condition such as the leakage current in IDDQ testing or the transient current in IDDT analysis. In case of hardware Trojan detection the output of the current sensor is compared with a reference value to provide a single bit logic output reflecting whether the circuit successfully passes the test. Although these built-in current sensors ha small footprint they cannot provide with sufficient data to be utilized as a power signature to diagnose IoT aberrant activity. An on-chip low-voltage current-sensing circuit has been developed for CMOS buck power converters which provide overcurrent protection and improve efficiency. The sensing accuracy is higher than 94% which is verified along with the effectiveness in current-mode operation and stability of the power converter by applying the proposed circuit to a buck regulator [41]. But the circuits are very complicated and the outputs are not digitized [21].

A current sensor has been built which is different from other existing ones as it fits in IoT device cost, size and power consumption constraints as well as provides the output in digital format. This sensor presents a design that integrates the power signature capture function into LDO regulators, which have been widely used to regulate the supply voltages of various components of the IoT devices and the digitized data can be conveniently analyzed by a software procedure which is executed by the microcontroller or microprocessor of the IoT device immediately after the completion of an operation. Experiments are carried out to demonstrate the potential of using the power-signature-based method to detect IoT operation anomalies, such as altered RF transmission levels, sabotaged sensor sampling rates, or unintended microcontroller peripheral activities [21, 22]. The shortcoming of this circuit is the minimum required capacitor size is 2.33nF which gives a large off-chip capacitance resulting in a large footprint on the circuit board.

CHAPTER 3

PROPOSED CURRENT TO DIGITAL CONVERSION TECHNIQUES

In this chapter, we propose two methods to generate digital code as the power signature of IoT device current consumption. Both methods assume the current to be measured have been sampled by other circuits and the sampled currents are represented current sources, I_{in} in the discussion. Also, both methods require a reference current source I_{ref} with whom the input current source is compared. In the first method, the value of all possible I_{in} is required to be smaller than I_{ref} and the generated code is the digital representation of the analog value as a conventional analog to digital converter (ADC). The second method allows I_{in} to be larger than I_{ref}. It extends the range of input current to be measured. But the linear relation between the generated digital code and the analog current value is sacrificed and the method suffers from accuracy degradation with the increase of I_{in} values.

3.1 PROPOSED METHOD 1

The block diagram of the first proposed method for the acquisition of power signature is shown in Figure 3.1. In this method the input current source, I_{in} is copied by a current mirror circuit which is consisted of M_3 and M_4 P-type transistors. The copied currents are used to charge node b constantly. Similarly, reference current I_{ref} is copied by a current mirror circuit which is consisted of M_1 and M_2 N-type transistors. A dc battery, V_a is connected to one of the input nodes of a comparator and the voltage of b node, V_b is connected to the other input node. The current flowing from the input source charges the capacitors C for the whole time period of the circuit operation. Depending on the comparator output, the copied reference either continues to discharge or does not continue to discharge the node b. This operation is achieved by via a switch S. The comparator output, V_{comp} is fed into a DFF. The DFF output controls the states of the switch, S. DFF will only change the outputs in the rising edge of clock cycle. When the capacitor is charging the output of the DFF becomes zero at the rising edge of the clock. Now, when the capacitor starts discharging it does not change the control signal immediately, as the DFF waits to change the signal for the rising edge of clock cycle. And this process continues for the total So, the duration of clock cycle for the charging and discharging process will be equal. Also, this comparator output signal is used as the enable signal of an n-bit counter. The counter is enabled only when the enable input is low and it freezes the output value after $N= 2^n$ clock cycles. Thus, this counter counts how many times the comparator output becomes zero.

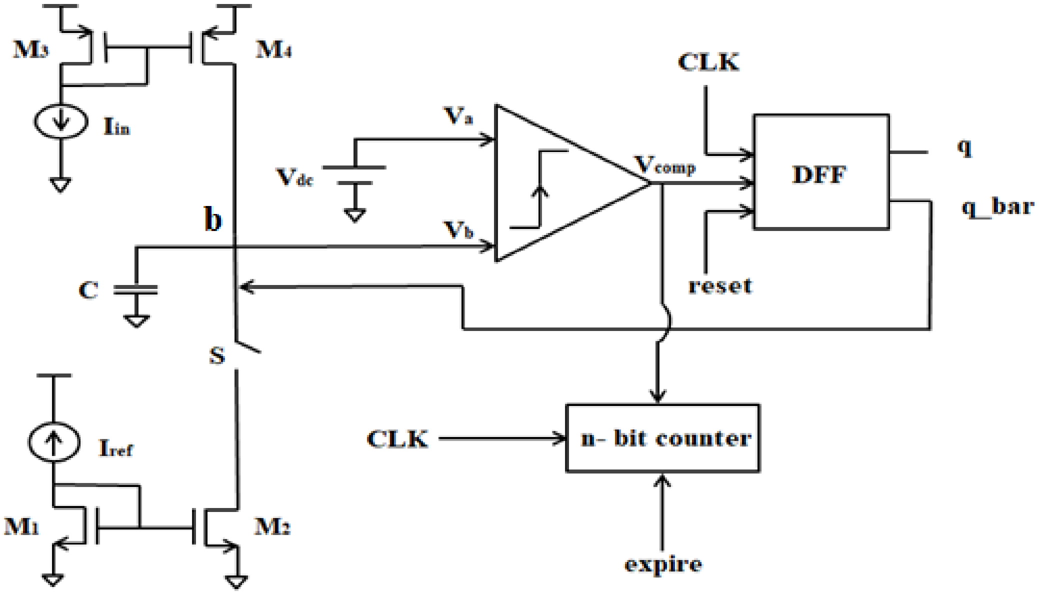

Figure 3.1 Block Diagram of the 1st Proposed Method

The operation of the proposed method is explained as follows. When V_a is greater than V_b, the output of the comparator, V_{comp} is high. So, the outputs of the DFF, q and q_bar become high and low respectively. Now, q_bar is fed back to the switch. In every rising edge of the clock cycle, when V_{comp} becomes high (i.e., 1) it opens the switch. Then, capacitor, C attached to node b stops to be discharged through I_{ref} resulting in an increment of V_b. So, V_a becomes low & V_b

becomes high. When, V_{comp} becomes low (i.e., 0) the outputs of the DFF, q and q_bar become low and high respectively. Now, control signal q_bar closes switch, S. At this time, capacitor C discharges through I_{ref}. So, the voltage at node b, V_b starts to decrease resulting in a high signal at the output node of the comparator. Such operation was performed for N clock cycles. The V_{comp} signal goes to the counter. The waveforms of the operation are shown in figure 3.2.

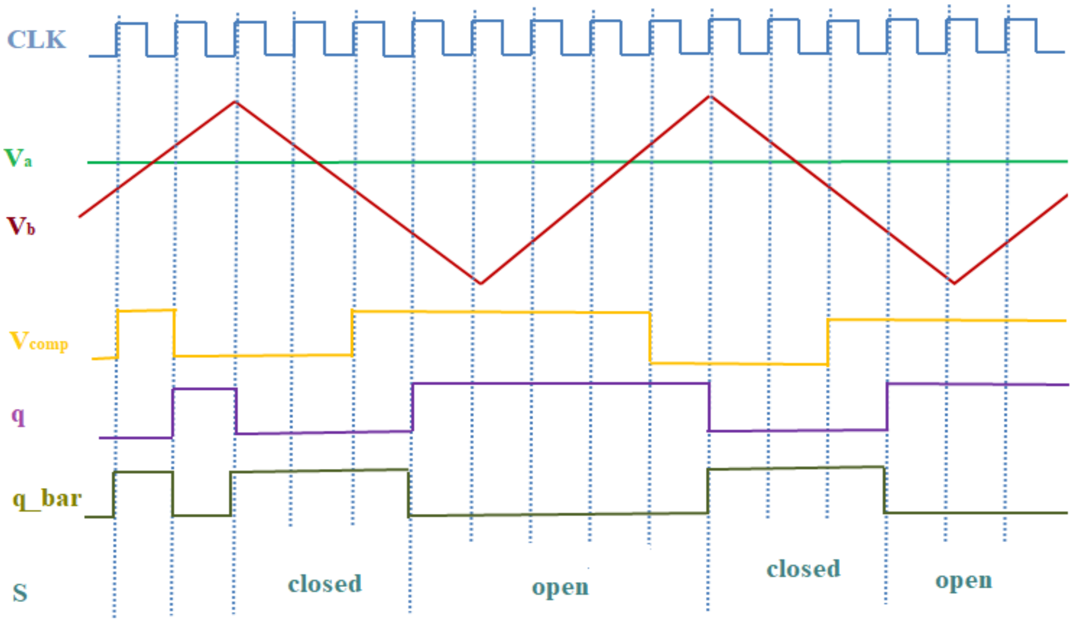

Figure 3.2 Operation of the 1st Proposed Method

In the process of converting the current value to a digital code, I_{ref} and N are fixed parameters; M is the counter value at the end of the conversion. The expression of I_{in} in terms of I_{ref}, N, and M are derived as follows. For the convenience of discussion, we use T_s to denote the clock period. During the conversion process, capacitor C is charged by I_{in} for N clock cycles and discharged by I_{ref} by M clock cycles. After this process, the residue charge Q_r at C can be found by the following equation,

$$Q_r = I_{in} \cdot N \cdot T_s - I_{ref} \cdot M \cdot T_s \qquad (1)$$

From the above equation, we can solve for I_{in} as:

$$I_{in} = I_{ref} \cdot \frac{M}{N} + \frac{Q_r}{N \cdot T_s} \qquad (2)$$

The first term on the right side of the equation represents the digital code of the analog value of input current. The second term is an error term caused by the residue charge Q_r. If N is very large, the magnitude of the error term becomes small and hence we can ignore it. Thus, we have:

$$I_{in} = I_{ref} \cdot \frac{M}{N} = I_{ref} \cdot \frac{M}{2^n} \qquad (3)$$

We can clearly see that, for this approach N must be very larger than M. This means the charging period of the capacitors needs to be larger. That will happen when I_{in} will be smaller and will take greater amount of time to make the capacitors charged. This implies that this method keeps linearity but requires a larger reference current source than all possible input current sources. For power signature analysis, we do not need an exact value. Only a related value to circuit operation can provide with the desired contribution. Therefore, nonlinearity can be tolerated. Thus, we proposed the second method without any boundaries for the value of the input and reference current sources.

3.2 PROPOSED METHOD 2

The block diagram of the second proposed method for the acquisition of power signature is shown in Figure 3.3. The input current source, I_{in} is copied by a current mirror circuit which is consisted with M_3 and M_4 P-type transistors and this time the mirrored current is connected to the node b via S_2 switch. The reference current source I_{ref} is copied by a current mirror circuit which is consisted with M_1 and M_2 N-type transistors and connected to the node b via S_1 switch just as the first method. So, the currents flowing from both current sources to and from the node b depend on the opening and closing states of these two switches. When S_1 is closed capacitor C discharges via I_{ref} and when S_2 is closed it discharges via I_{ref}. According to these operations the voltage at node b increases or decreases. A dc battery, V_a is connected to one of the input nodes of a comparator and the voltage of b node, V_b is connected to the other input node. The comparator output, V_{comp} is fed into a DFF. The DFF output controls the states of the switches S_1 and S_2. Also, this comparator output signal is used as the enable signal of an n-bit counter. The counter is enabled only when the enable input is low and it freezes the output value after *N= 2ⁿ* clock cycles. Thus, this counter counts how many times the comparator output becomes zero.

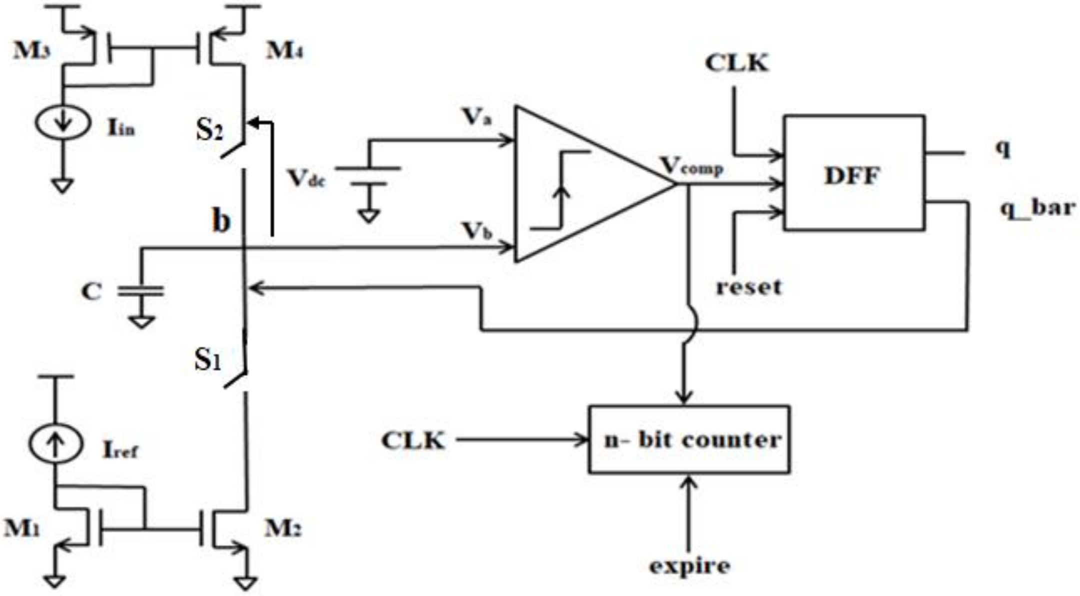

Figure 3.3 Block Diagram of the 2nd Proposed Method

The operation of the proposed method is explained as follows. When V_a is greater than V_b, the output of the comparator, V_{comp} is high. So, the outputs of the DFF, q and q_bar become high and low respectively. Now, q_bar is fed back to the switch S_1 and S_2. In every rising edge of the clock cycle, when V_{comp} becomes high (i.e., 1) it opens S_1 and closes the switch S_2. Then, capacitor, C attached to node b starts to be charged by I_{in} and stops to be discharged through I_{ref} resulting in an increment of V_b. So, V_a becomes low & V_b becomes high. Then, V_{comp} becomes low (i.e., 0) the outputs of the DFF, q and q_bar become low and high respectively. Now, control signal q_bar closes switch, S_1 and opens S_2. At this state, the capacitor starts charging by I_{in} and discharging through I_{ref}. So, the voltage at node b, V_b starts to decrease resulting in a high signal at the output node of the comparator. Such operation was performed for N clock cycles. The V_{comp} signal goes to the counter. The waveforms of the operation are shown in figure 3.4.

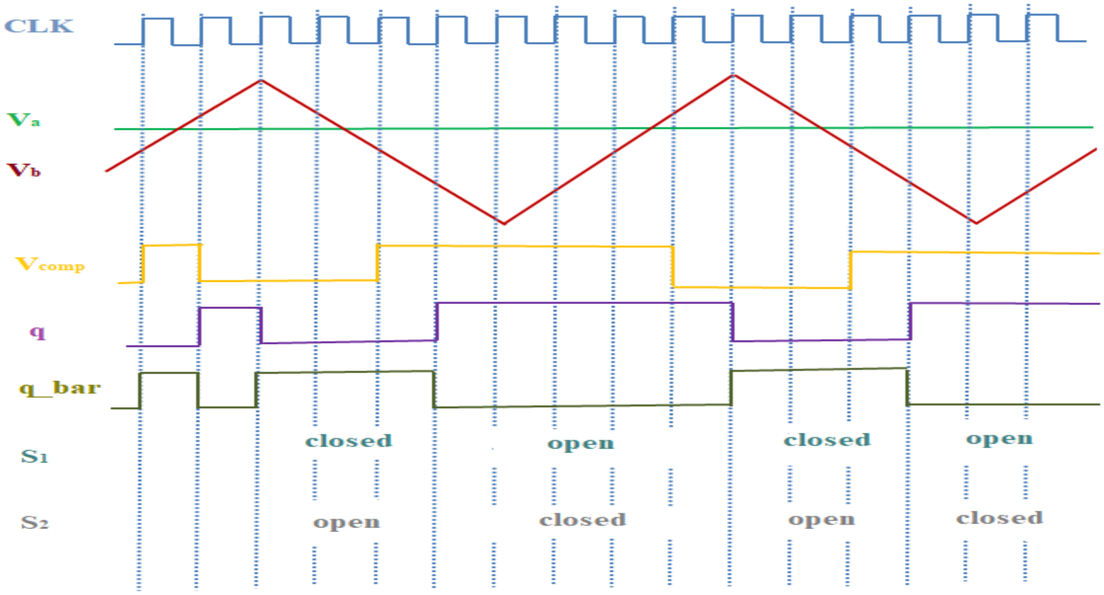

Figure 3.4 Operation of the 2nd Proposed Method

In the process of converting the current value to a digital code, I_{ref} and N are fixed parameters also; M is the counter value at the end of the conversion. The expression of I_{in} in terms of I_{ref}, N, and M are derived as follows. For the convenience of discussion, we use T_s to denote the clock period. During the conversion process, capacitor C is discharged by I_{ref} for M clock cycles and charged by I_{in} by $(N - M)$ clock cycles. After this process, the residue charge Q_r at C can be found by the following equation,

$$Q_r = I_{in} \cdot \ (N - M) \cdot T_s - \ I_{ref} \cdot M \cdot T_s \tag{4}$$

We can solve for I_{in} as:

$$I_{in} = \ I_{ref} \cdot \frac{M}{N-M} + \frac{Q_r}{(N-M) \cdot T_s} \tag{5}$$

If the term $(N - M)$ is very large we can ignore the expression $\frac{Q_r}{(N-M)\cdot T_s}$. From that we can get expression of I_{in} as

$$I_{in} = I_{ref} \cdot \frac{M}{N-M} \tag{6}$$

However, if N and M are close then the equation (6) will not be very accurate, and the error value will be appeared with the input current source value.

$$I_{in} = I_{ref} \cdot \frac{M}{N-M} + \mathcal{E} \tag{7}$$

$$\mathcal{E} = \frac{\mathrm{Q_r}}{(N-M)\cdot T_s} \tag{8}$$

We can estimate the inaccuracies by the above error term with the following circuit parameters: clock period $T_s = 10\ ns$, $C = 1.5\ pF$. Since $Q_{r,max} = C \cdot V_{d,max}$, where $V_{d,max}$ is the maximum voltage difference between nodes a and b at the end of the conversion process. Because $I_{in} > I_{ref}$, $V_{d,max}$ occurs in the case that V_a is only slightly smaller than V_b at the end of the second from the last conversion cycle and I_{in} charges node a during the last conversion cycle. Hence, $V_{d,max}$ can be estimated as:

$$V_{d,max} \approx \frac{I_{in}\cdot T_s}{C} \tag{9}$$

This indicates that $Q_{r,max} = I_{in} \cdot T_s$. Substituting this relation to equation 7, we have:

$$I_{in} = I_{ref} \cdot \frac{M}{N-M} + \frac{I_{in}}{(N-M)} \tag{10}$$

From the above equation, we can solve for M in terms of I_{in}, I_{ref}, N.

$$M = f(I_{in}, I_{ref}, N) = \frac{I_{in}\cdot(N-1)}{I_{in}+I_{ref}} \tag{11}$$

Substituting the expression for M and $Q_{r,max} = I_{in} \cdot T_s$ into the equation 8, we can get the following error term expression.

$$\mathcal{E} = \frac{I_{in}\cdot(I_{in}+I_{ref})}{N\cdot I_{ref}+I_{in}} \tag{12}$$

So, the relative error value is:

$$E = \frac{(I_{in} + I_{ref})}{N \cdot I_{ref} + I_{in}} \tag{13}$$

To analyze the relative error value a MATLAB code was written for the range of 1µA- 200µA for I_{in} and for I_{ref}=50µA for different number of total clock cycle 1024, 2048 and 4096.

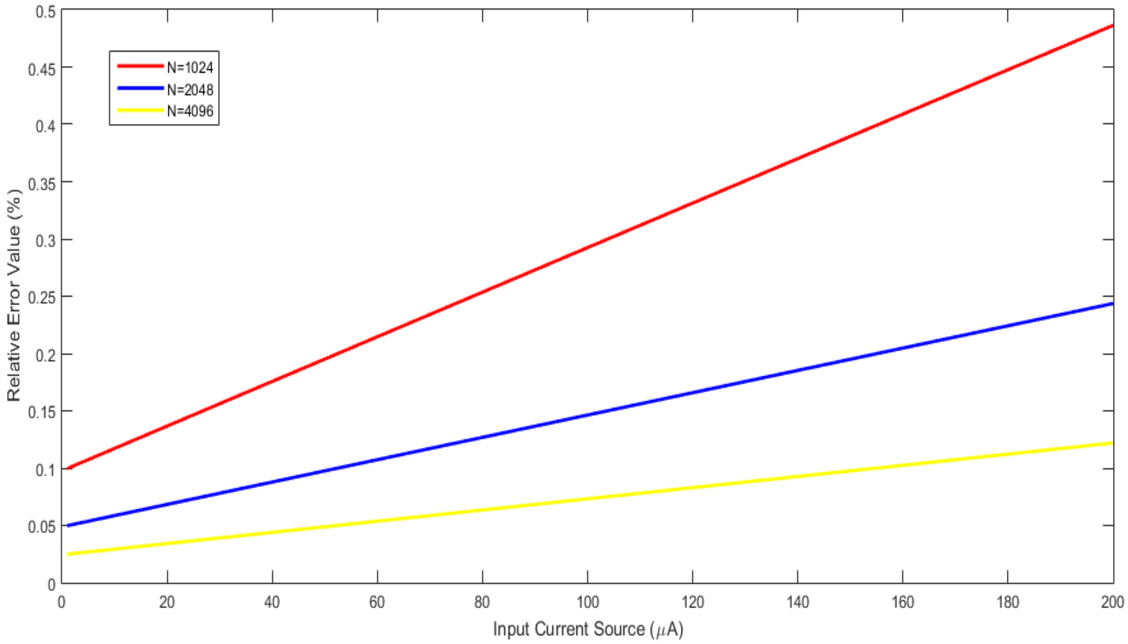

Figure 3.5 Output Error at Different Input Current Levels Considering Excess Charge in Capacitor

Observing the plot, we can see that with the increase of I_{in} the error increases for the same I_{ref}. As the more the I_{in} is increasing it is taking more smaller number of clock cycle to charge the capacitor and greater number of clock cycles to discharge the capacitor. So, $(N - M)$ is decreasing. Hence, equation (8) is proving that the error will increase. Also, if we increase the number of clock cycle for the whole operation the value of error decreases. As, in this way N is bigger so the term $(N - M)$ becomes larger which is desirable to have smaller value of error. The graph shows the worst-case scenario. The real operation will have less amount of error.

3.4 ANALYSIS OF RESIDUE CHARGE Q_r

There will be residue charge at the nodes for two reasons. One is due to offset voltage, V_{os}. The internal structure of a comparator contains a differential amplifier which should have two identical transistors. That is why for ideal op-amp if both the inputs are grounded the output will be zero volt. But, for real op-amp there is found some finite voltage at the output terminal which is called offset voltage. This offset voltage is the voltage required to be provided to the input in order for the output to be zero. Offset voltage is caused by a disparity in the biasing voltage between the base-emitter of the differential input transistors (the gate-source voltage mismatch in FET-input amplifiers) [42]. Also, an additional voltage, $V_{d,max}$ will be present at the node in the case that I_{in} charges node b during the last conversion cycle. For this, the charge will be, $Q_{r,max} = I_{in} \cdot T_s$.

So. The total residue charge at node b will be the summation of these two charges. i.e.

$$Q_r = C \cdot V_{os} + I_{in} \cdot T_s \tag{14}$$

Putting this value of Q_r in equation 8, we get the error value expression as,

$$\mathcal{E} = \frac{C \cdot V_{os} + I_{in} \cdot T_s}{(N-M) \cdot T_s} \tag{15}$$

Putting this error value in equation (7) an expression for I_{in} can be found,

$$I_{in} = \ I_{ref} \cdot \frac{M}{N-M} + \frac{C \cdot V_{os}}{(N-M) \cdot T_s} + \ \frac{I_{in}}{N-M} \tag{16}$$

Solving this we can get an expression for M,

$$M = \frac{T_s \cdot I_{in}\,(N-1) - \ C \cdot V_{os}}{T_s \cdot \,(I_{in} + I_{ref})} \tag{17}$$

Substituting the expression for M and Q_r into the equation 8, we can get the following error term expression,

$$\mathcal{E} = \frac{(C \cdot V_{os} + I_{in} \cdot T_s) \cdot (I_{in} - I_{ref})}{T_s \cdot \left(I_{in} + N \cdot I_{ref}\right) + C \cdot V_{os}} \tag{18}$$

So, the relative error value is,

$$E = \frac{(C \cdot V_{os} + I_{in} \cdot T_s) \cdot (I_{in} - I_{ref})}{I_{in} \cdot [T_s \cdot (I_{in} + N \cdot I_{ref}) + C \cdot V_{os}]} \tag{19}$$

We can analyze the inaccuracies by the above error term with the following circuit parameters: clock period $T_s = 10\ ns$, $C = 1.5\ pF$ and comparator off-set voltage $V_{os} = 250\mu V$. A MATLAB code was written for the range of 1μA- 200μA for I_{in} and I_{ref}=50μA assuming the for different number of total clock cycle 1024, 2048 and 4096.

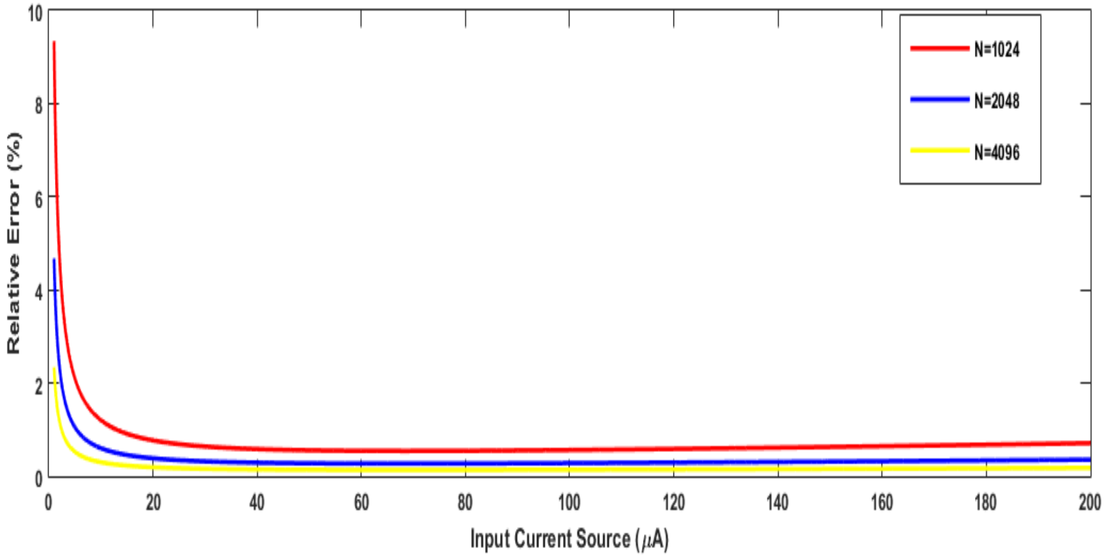

Figure 3.6 Output Error at Different Input Current Levels Considering Excess Charge in Capacitor and Offset Voltage of Comparator

This plot is justifying equation (18) as in the denominator there is the term I_{in}, which means if I_{in} increases it gives a large value at the denominator of the equation lowering the ultimate value of the error term. The real operation may have different values for the error as this plot is based on an estimated offset voltage of the comparator and a specific value of the capacitor and clock frequency. The error can be minimized by choosing optimum values of these factors for different conditions.

CHAPTER 4

CIRCUIT IMPLEMENTATION AND SIMULATION RESULTS

This chapter will discuss the circuit Design and operation for the proposed method along with the investigation of the effectiveness of these circuit setups through the investigation of the simulation results at various operation conditions. The implemented circuits are designed using commercial 130 nm CMOS technology. For both method we constructed two current mirror circuit for I_{in} and I_{ref}. A circuit of feedback loop is setup to determine how the control circuitry behaves as control circuitry is needed to determine which transistors are turned on. To implement both methods we setup two different circuit setups for getting feedback signals. In one setup we used a latch-based comparator to compare the voltage of the node connected to a capacitor with a DC voltage. In another circuit setup, an inverter is designed which plays the role of a comparator. A DFF is assembled in the circuits to control the states of the circuits and a Verilog-a counter is employed to generate digital code as the power signature of IoT device current consumption. Finally, we will investigate the simulation results for a wide range of input current sources for all the circuit setups to evaluate the performance of the designed circuits.

4.1 COMPARATOR DESIGN

A latch-based comparator showed in figure 4.1 is used to achieve feedback signal to control the switches in the circuit setup to capture power generation. When the comparator output is logic 0, this indicates the output voltage is too low and when the output is logic 1, this indicates the output voltage is too high. This means the comparator output can be directly used as the feedback control signal. Since the comparator only changes with a rising edge of the system clock, it will have the same logic value through both phases of a single clock, which is needed. This comparator is consisted of an analog MOSFET circuit and a digital logic gate circuit setup.

The comparator is designed with 3.3V device technology. The 3.3V devices have thick gate oxide layers to enable them to tolerate 3.3V voltage. The voltage levels of majority of the devices are 5 V to guarantee universal compatibility. However, as technology is evolving, similar devices have been developed that consume less power and function at a lower base voltage (V_{cc}= 3.3V as contrast to 5V). For 3.3V devices, there is a slight difference in the manufacturing processes, which results in a more compact design and reduced system costs. It doesn't necessitate any extra parts to interconnect a 3.3V device to a 5V device. Logic 1 (HIGH), for instance, will be at least 2.4V when coming from a 3.3V device. Given that it is over the 2V threshold voltage, this will still be read as a logic 1 (HIGH) to a 5V system [43].

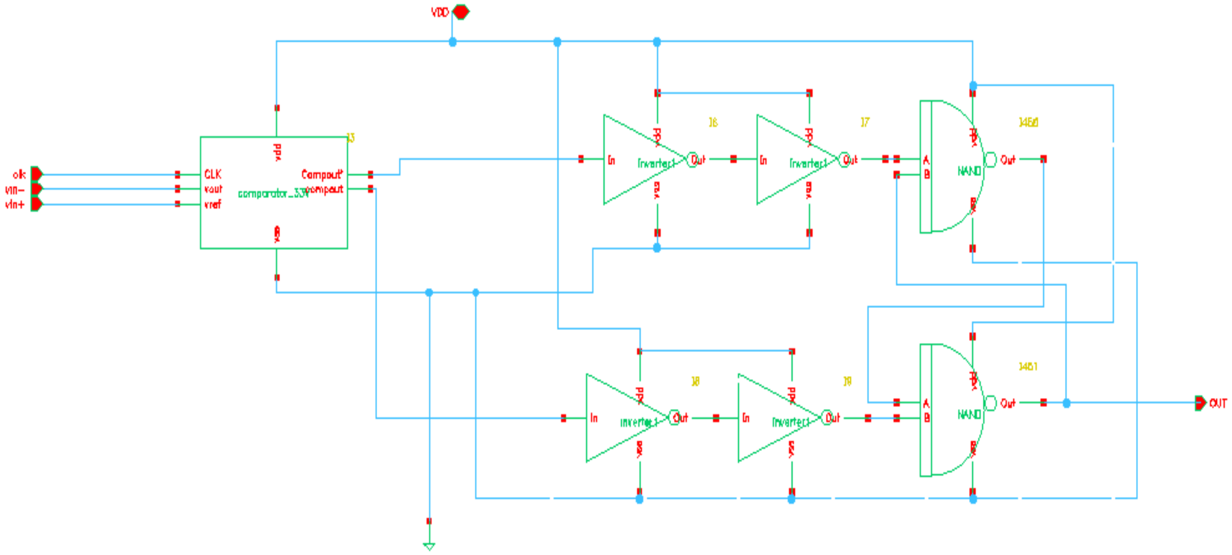

Figure 4.1 The Comparator Circuit

In figure 4.1, we can see a block named comparator_33V. The block is the symbol used for the circuit built with MOSFETs of figure 4.2. This analog circuit contains two latches to generate the desired result at the output node of the comparator. The function of this circuit can be stated as follows. At initial state, assume clock is low and $V_{out} > V_{ref}$. So, transistors T_0, T_1, T_8 and T_9 gets turned on, T_5 is turned on as V_{out} is high and T_{12} is off as V_{ref} is low. This state makes $compout$ & $compout'$ and the nodes x & y high. Now when clock rises transistors T_0, T_1, T_8 and T_9 gets turned off. As $compout$ and $compout'$ are high, the gate voltage of transistors T_{13} and T_{14} are high making those closed. Also, high clock makes the T_{15} closed. So, this state discharges $compout'$ via closed T_5 lowering it. As T_{12} is closed $compout$ cannot be discharged. So, it remains high. The opposite operation takes place when $V_{ref} > V_{out}$. For the shake of simplicity, all the transistors used in the circuit have the same size. The size of PMOS is W/L=1000nm/400nm. For NMOS the size W/L= 500nm/400nm is chosen. In comparators, large gain is desired. A considerable gain is desirable in comparators. Better gain is attainable with a greater channel length than with a smaller one. Furthermore, devices with shorter channel lengths are less resistant to process fluctuations, which are essential for achieving a high yield. [44]. That is why for this comparator design transistors with minimum channel length are not used.

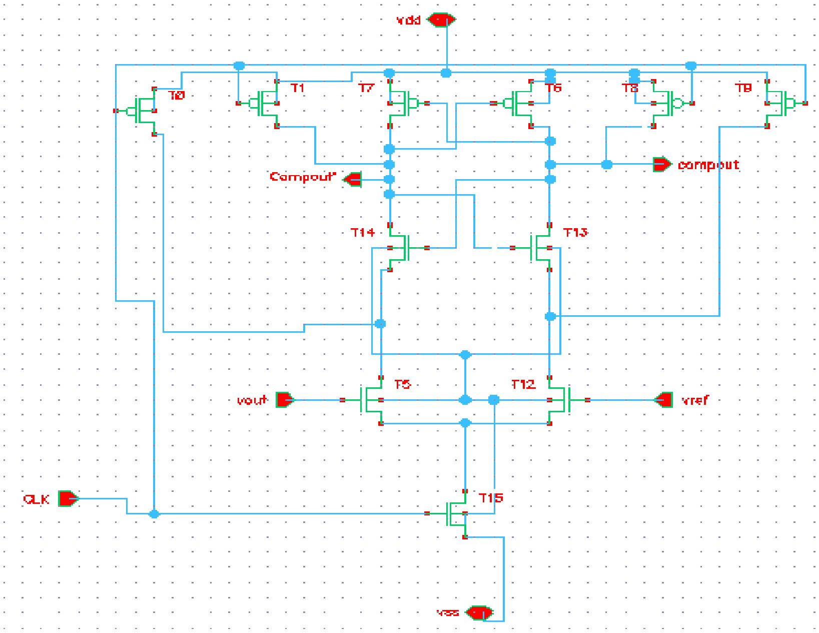

Figure 4.2 MOSFET Circuit Used in Comparator

The digital logic circuit is designed in such a way that the assembled circuit of the analog and digital setup compares the comparator inputs, V_{in}^{+} and V_{in}^{-} and changes the output at the rising edge of the clock. To justify the operation of the comparator a simulation result is exhibited in figure 4.3. This result justifies the operation of having a high output when $V_{in}^{+} > V_{in}^{-}$ and vice versa. This comparator can give accurate output for the difference of 0.01V. As we can see when V_{in}^{+} is 1.66V and V_{in}^{-} is 1.65V the V_{comp} is low on the rising edge of clock.

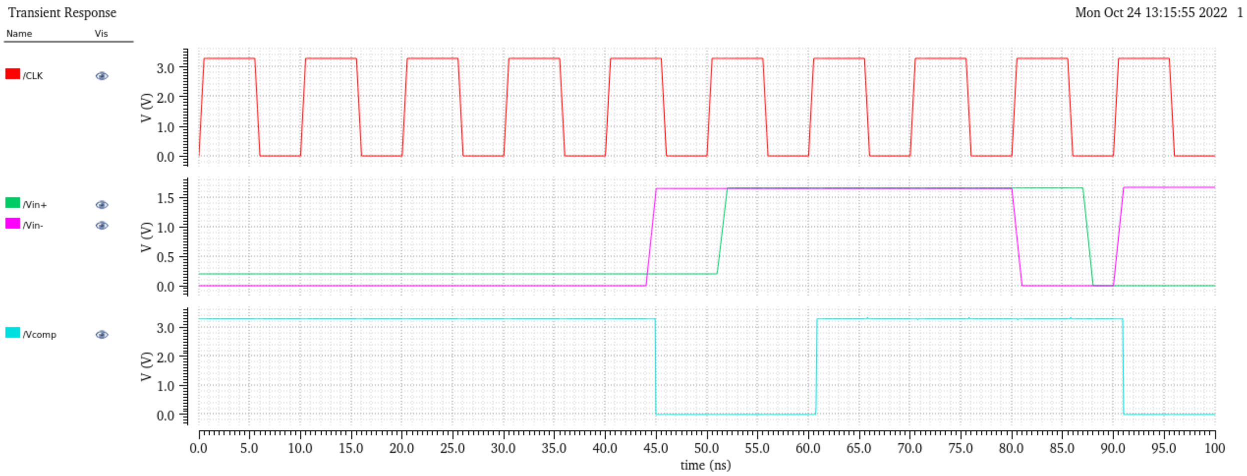

Figure 4.3 Simulation Result of the Comparator

4.2 CIRCUIT IMPLEMENTATION OF 1ST PROPOSED METHOD WITH LATCH-BASED COMPARATOR

The circuit design of the first proposed method for the acquisition of power signature is shown in Figure 4.4. The input current source, I_{in} is copied by a current mirror circuit which is consisted with T_0 and T_1 PMOS and this time the mirrored current is connected directly to the node b. The reference current source I_{ref} is copied by a current mirror circuit which is consisted with T_6 and T_7 NMOS and connected to the node b via T_5 switch. So, the currents flowing from both current sources to and from the node b depend on the opening and closing states of these two transistors which are working as switches. When T_5 is closed capacitor C discharges via I_{ref}

and when T_3 is closed it discharges via I_{ref}. According to these operations the voltage at node b increases or decreases. A dc battery, V_a is connected to one of the input nodes of a comparator and the voltage of b node, V_b is connected to the other input node. The comparator output, V_{comp} is fed into the DFF. The DFF output controls the states of the switches T_3 and T_5. Also, this comparator output signal is used as the enable signal of an n-bit counter. The counter is enabled only when the enable input is low and it freezes the output value after *N=1024* clock cycles. Thus, this counter counts how many times the comparator output becomes zero.

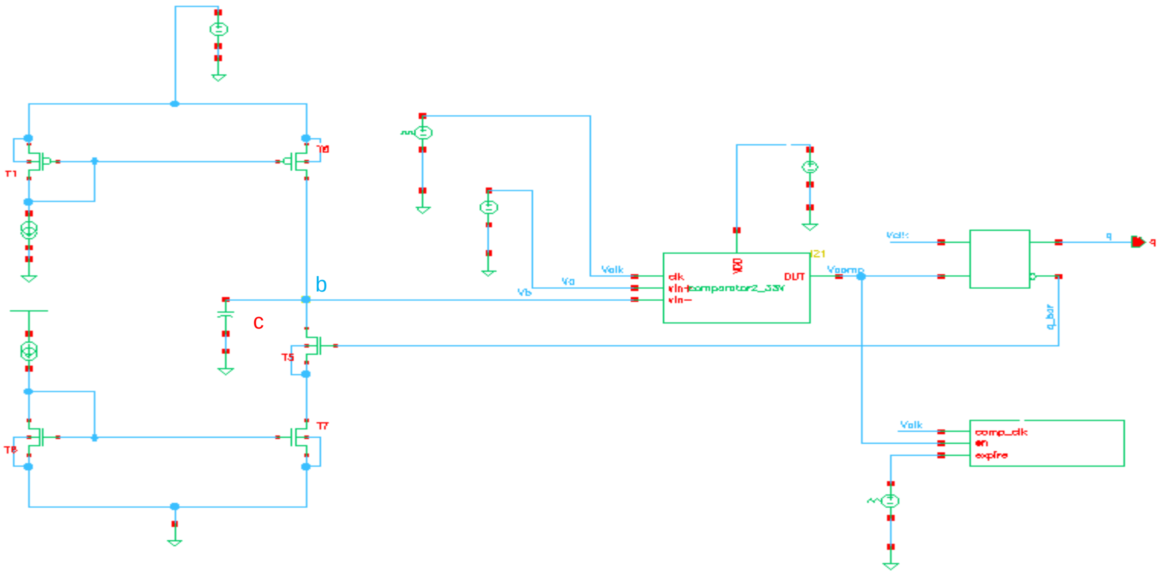

Figure 4.4 Circuit Implementation for 1st Proposed Method with Comparator

For the current mirror circuit, a size of $\frac{W}{L} = 10\mu m/1.2\mu m$ PMOS and a size of $\frac{W}{L} = 2\mu m/1.2\mu m$ NMOS were chosen. Long channel length is influenced by both the current mirror's electrical characteristics and its design. In the electrical field larger length will stabilize the current by lowering the channel length modulation and increasing the output resistance of the current mirror. Because of variance on the wafer will be averaged over the long channel while it is concentrated in the tiny channel, this results in significantly different qualities between the small channel transistors in terms of physical (layout) properties compared to the big channel [45]. The multiplicity of transistors is three. That means three parallelly connected MOSFETs are used to form the current mirror circuit. The parallel connection of switches hence, MOSFETs has the purpose of dividing the powers involved and creating devices that can withstand greater power. If a single transistor is insufficient to control the current, transistors can be employed in parallel. The current handling capacity may be better managed with more parallel transistors, which also avoids harm from being done to any one transistor [8]. The sizing of the capacitors is not a trivial matter. They must be large enough that the channel charge injection is negligible, otherwise the relationship established will not be accurate. A 1.5pF capacitor is used in this setup. Depending on the size of capacitor the duration of cycles for charging and discharging will be changed.

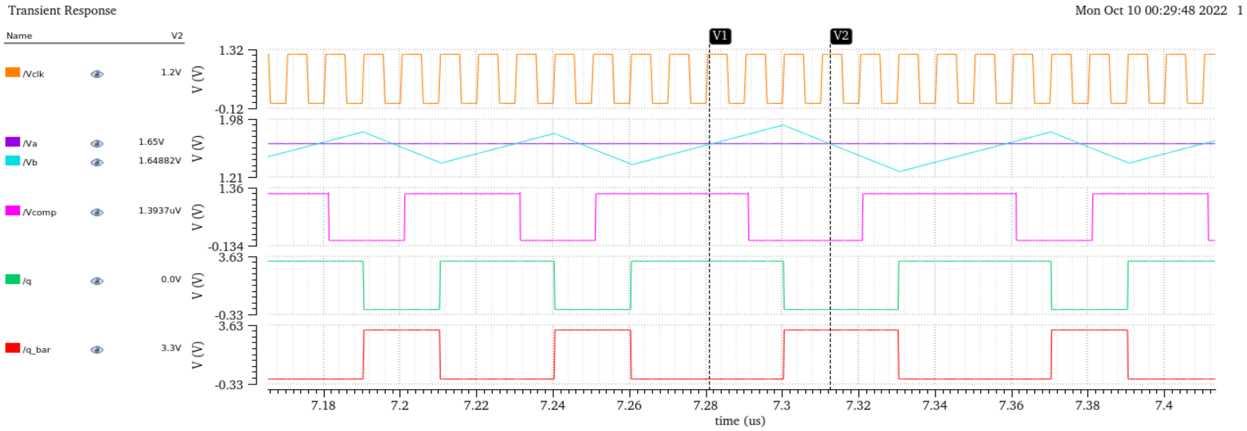

Figure 4.5 Simulation of the Circuit for 1st Proposed Method with Comparator ($I_{ref} > I_{in}$)

The operation of this circuit can be explained as follows. When V_a is greater than V_b and the clock cycle rises, V_{comp} becomes high. So, the outputs of the DFF, q and q_bar become high and low respectively. Now, q_bar is fed back to the T_5 switch. As q is low it turns off the transistor and hence the switch is open. Then, capacitor, C attached to node b stops to be discharged through I_{ref} resulting in an increment of V_b. So, V_a becomes low & V_b becomes high.

When, V_{comp} becomes low (i.e., 0) the outputs of the DFF, q and q_bar become low and high respectively. The high q_bar turns on the transistor . Hence, the switch is closed. At this time, capacitor C discharges through I_{ref}. So, the voltage at node b, V_b starts to decrease resulting in a high signal at the output node of the comparator. The V_{comp} signal goes to the veriloga counter. The counter is enabled when the V_{comp} is low and counts the number of zero at the enable port for 1024 clock cycles. The simulation result for $I_{ref} = 50\mu A$ & $I_{in} = 20\mu A$ i.e., $I_{ref} > I_{in}$ is displayed in figure 4.5. For this condition the waveforms follow as the operation is stated.

Several simulations are conducted for different values of $I_{in} < 50\mu A$ and $I_{ref} = 50\mu A$ i.e., $I_{ref} > I_{in}$ for 1024 and 2048 clock cycles where one clock period $T_s = 10ns$. Using the equation (3) we can calculate the value of I_{in}. We wrote a MATLAB code to plot a graph for the inaccuracy between the real value and the calculated value.

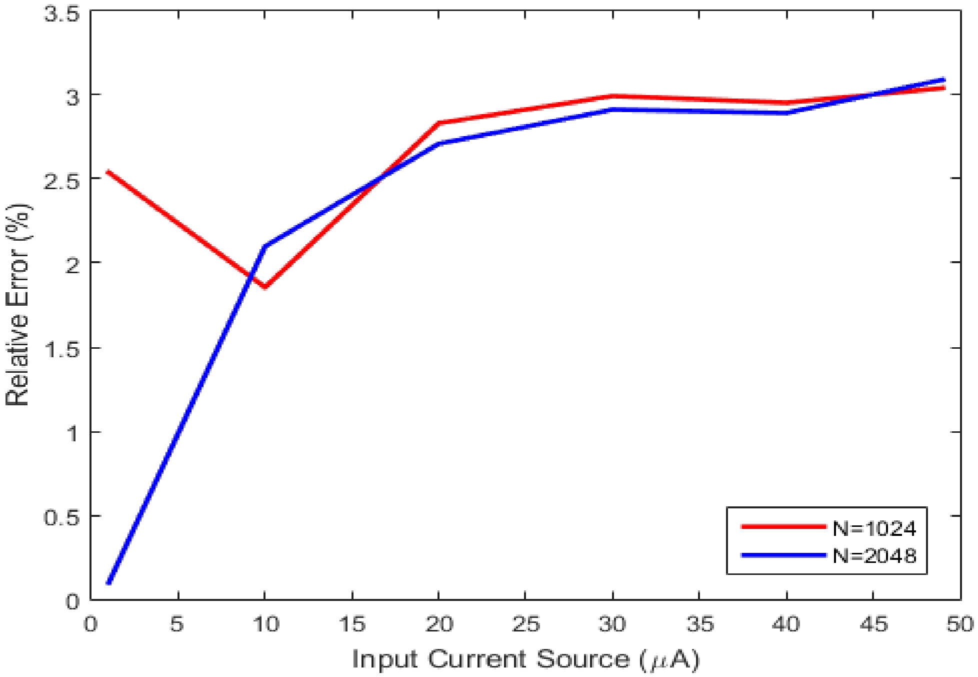

Figure 4.6 Relative Error vs Input Current Curve for 1st Method Implemented with Comparator

If we compare this plot with the plot of figure 3.5, we found by plotting the relative error equation (13) with different input current source value for $I_{ref} = 50\mu A$ where $I_{ref} > I_{in}$ we can find the justification from the simulation result that if the I_{in} increases the error increases. The more the value of input current source is closer to the value of reference current source the error in the result increases. And when input current value exceeds the reference current value i.e., $I_{ref} < I_{in}$ this method does not work. Because, as the capacitor is always getting charged, if I_{ref} is not greater than I_{in} the capacitor will never be discharged even when the switch is closed. Hence, there will be no discharging clock cycle. And the equation (3) cannot be evaluated hence no input current source value can be calculated from this method. Also, for bigger number of clock cycle for the whole operation the relative error is less if we compare the red line and the blue line of the plot. Which justifies the conclusion of this method.

4.3 CIRCUIT IMPLEMENTATION OF 2ND PROPOSED METHOD WITH LATCH-BASED COMPARATOR

In this method we have current mirror circuits to copy I_{in} and I_{ref} like the first method. But for this circuit we will have two switches to connect the capacitor with the current mirror circuits. Depending on them the capacitor of the circuit gets charged or discharged. The circuit design of the second proposed method for the acquisition of power signature is shown in Figure 4.7. The input current source, I_{in} is copied by a current mirror circuit which is consisted with T_0 and T_1 PMOS and this time the mirrored current is connected to the node b via T_3 PMOS which works as a switch. The reference current source I_{ref} is copied by a current mirror circuit which is consisted with T_6 and T_7 NMOS and connected to the node b via T_5 NMOS switch. So, the currents flowing from both current sources to and from the node b depend on the opening and closing states of these two transistors which are working as switches. When T_5 is closed capacitor C discharges via I_{ref} and when T_3 is closed it discharges via I_{ref}. According to these operations the voltage at node b increases or decreases. A dc battery, V_a is connected to one of the input nodes of a comparator and the voltage of b node, V_b is connected to the other input node. The comparator output, V_{comp} is fed into the DFF. The DFF output controls the states of the switches T_3 and T_5. Also, this comparator output signal is used as the enable signal of an n-bit counter. The counter is enabled only when the enable input is low and it freezes the output value after *N=1024* clock cycles. Thus, this counter counts how many times the comparator output this counter counts how many times the comparator output becomes zero.

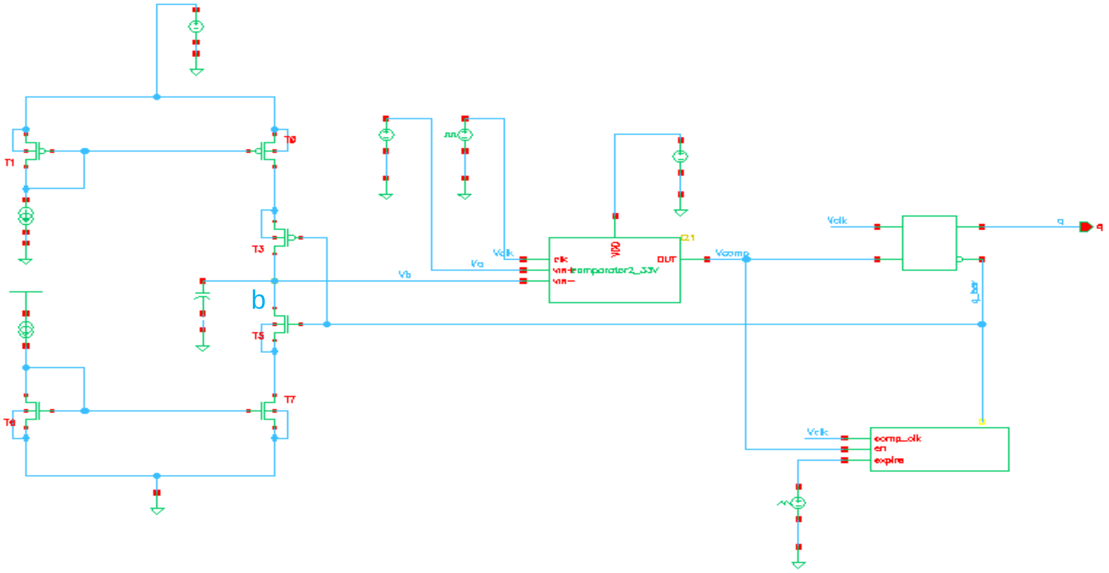

Figure 4.7 Circuit Implementation for 2nd Proposed Method with Comparator

The operation of this circuit can be explained as follows and can be justified by the simulation result of figure 4.10. When V_a is greater than V_b and the clock cycle rises, V_{comp} becomes high. So, the outputs of the DFF, q and q_bar become high and low respectively. Now, q_bar is fed back to the T_3 and T_5 switch. As q is low it turns on the switch T_3 and turns off the transistor T_5. Then, capacitor, C attached to node b starts to be charged by I_{in} and stops to be discharged through I_{ref} resulting in an increment of V_b. So, V_a becomes low & V_b becomes high.

When, V_{comp} becomes low (i.e., 0) the outputs of the DFF, q and q_bar become low and high respectively. As q is high it turns off the switch T_3 and turns on the transistor T_5. Then, capacitor, C attached to node b stops to be charged by I_{in} and starts to be discharged through I_{ref} resulting in a decrement of V_b. So, V_a becomes high & V_b becomes low. The V_{comp} signal goes to the veriloga counter. The counter is enabled when the V_{comp} is low and counts the number of zero at the enable port for the period of 1024 clock cycles. Figure 4.10 is the simulation result when $I_{ref} = 50\mu A$ & $I_{in} = 70\mu A$ i.e., $I_{ref} < I_{in}$ and it clearly shows that this circuit setup allows the I_{ref} to be smaller than I_{in}.

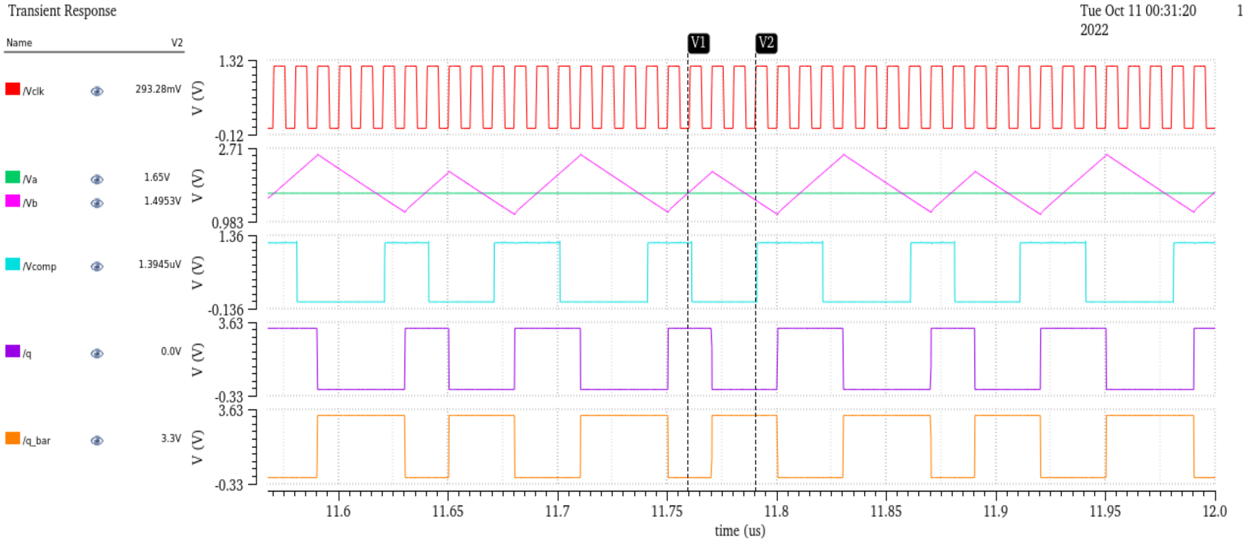

Figure 4.8 Simulation of the Circuit for 2nd Method with Comparator

The circuit's performance is analyzed by running the circuit with different load currents ranging from 1μA to 200μA where $I_{ref} = 50\mu A$ for 1024 and 2048 clock cycles. Here one clock period $T_s = 10ns$. Using the equation (10) we can calculate the value of I_{in}. We wrote a MATLAB code to plot a graph for the inaccuracy between the real value and the calculated value that is shown in figure 4.9.

Observing the plot, we can see that with the increase of I_{in} the error increases for the same I_{ref} as we found in the figure 3.5. As the more the I_{in} is increasing it is taking more smaller number of clock cycle to charge the capacitor and greater number of clock cycles to discharge the capacitor. So, $(N - M)$ is decreasing. Hence, equation (8) is proved. The error will increase dramatically after a certain increment in input current source value. Also, according to the equation, if the number of clock cycle for the whole operation is increased the value of error decreases. As, in this way N is bigger so the term $(N - M)$ becomes larger which is desirable to have smaller value of error. But, in the plot we can see that the errors are very close when simulated with different number of clock cycles. This is because of various simulation artifacts. The graph shows the worst-case scenario. The real operation will have less amount of error.

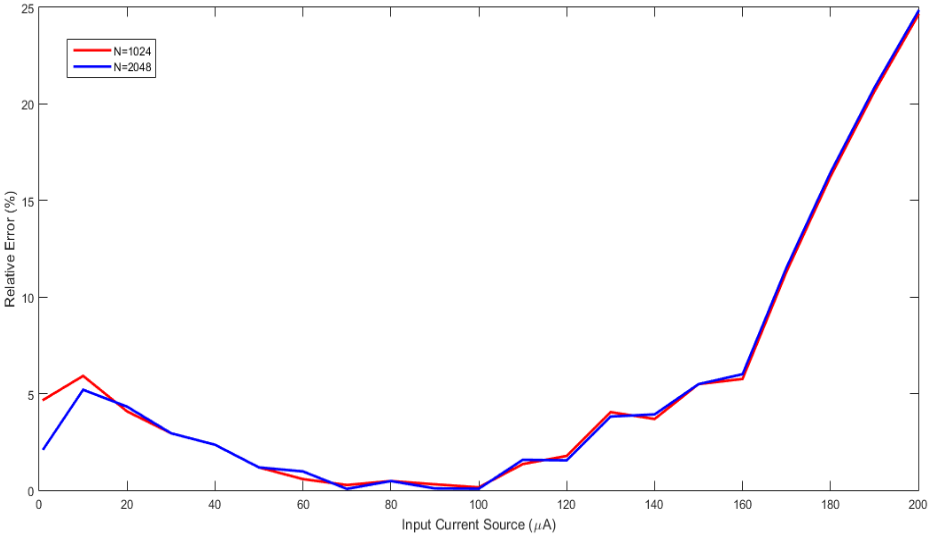

Figure 4.9 Relative Error vs Input Current Curve for 2nd Method Implemented with Comparator

4.4 INVERTER OPERATION

An inverter is designed to use in the circuit to control the switches with PMOS of size $\frac{W}{L} = \frac{2400nm}{400nm}$ and NMOS of size $\frac{W}{L} = \frac{1200nm}{400nm}$. An increased channel length is used to design the inverter to reduce delay. We connected several inverters in series to get proper stimulation to operate the DFF. The dc sweep simulation of three inverters connected in series is shown in figure 4.10. If we zoom in the graph, we can see that the inverter considers any signal above 1.65V as logic one and any signal below 1.6V as logic zero. That means this inverter cannot operate properly in between 1.6V to 1.65V as it cannot detect if the signal is logic high or logic low.

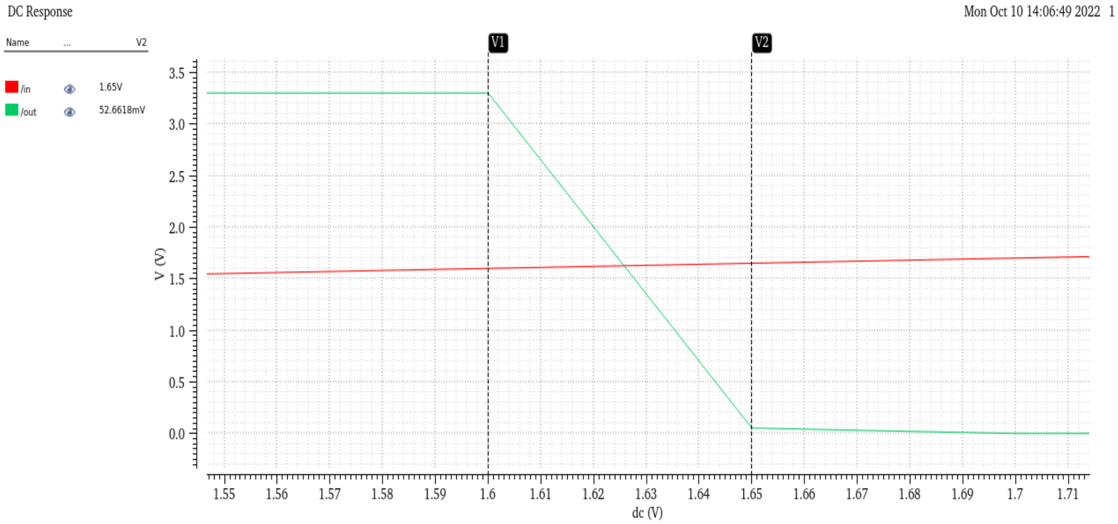

Figure 4.10 Zoomed in DC Sweep Simulated Voltage Transfer Curve

4.5 CIRCUIT IMPLEMENTATION OF 1ST PROPOSED METHOD WITH INVERTER-BASED COMPARATOR

For this circuit setup the switch control signals are generated based on the inverter output signal. The circuit sing the inverter for the first proposed method for the acquisition of power signature is shown in Figure 4.12. All the setup for this circuit is exactly the same of the circuit setup for the first proposed implemented with comparator except instead of a comparator three series connected transistors are used.

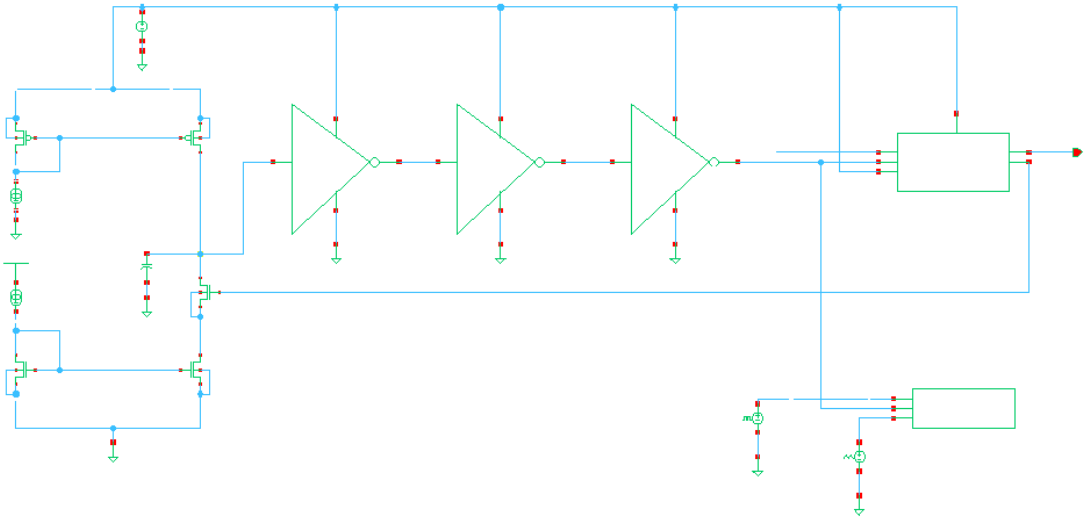

Figure 4.11 Circuit Implementation for 1st Proposed Method with Inverter

The operation of this circuit can be explained as follows. The node V_b is charging by I_{in} for the whole time of the operation as I_{in} is copied via a current mirror to this node. Now, whenV_{comp} is low on the rising edge of clock cycle the outputs of the DFF, q and q_bar become low and high respectively. Now, q_bar is fed back to the T_5 switch. As q_bar is high it turns on the transistor T_5. Hence, the capacitor, C attached to node b starts to be discharged through I_{ref}. So, V_b starts to decrease and at time when it is below 1.6V at the end of the series of inverters the V_{comp} becomes high. This phenomenon makes the outputs of the DFF, q and q_bar high and low respectively at the next rising edge of the clock cycle. Now, q_bar is low it turns off the transistor T_5. Hence, the capacitor stops to be discharged through I_{ref}. So, V_b starts to increase and at time when it is above the threshold voltage of the inverter, 1.65V at the end of the series of inverters the V_{comp} becomes high. The V_{comp} signal goes to the veriloga counter. The counter is enabled when the V_{comp} is low and counts the number of zero at the enable port for 1024 clock cycles. The simulation result for $I_{ref} = 50\mu A$ & $I_{in} = 20\mu A$ i.e., $I_{ref} > I_{in}$ is displayed in figure 4.5. For this condition the waveforms follow as the operation is stated.

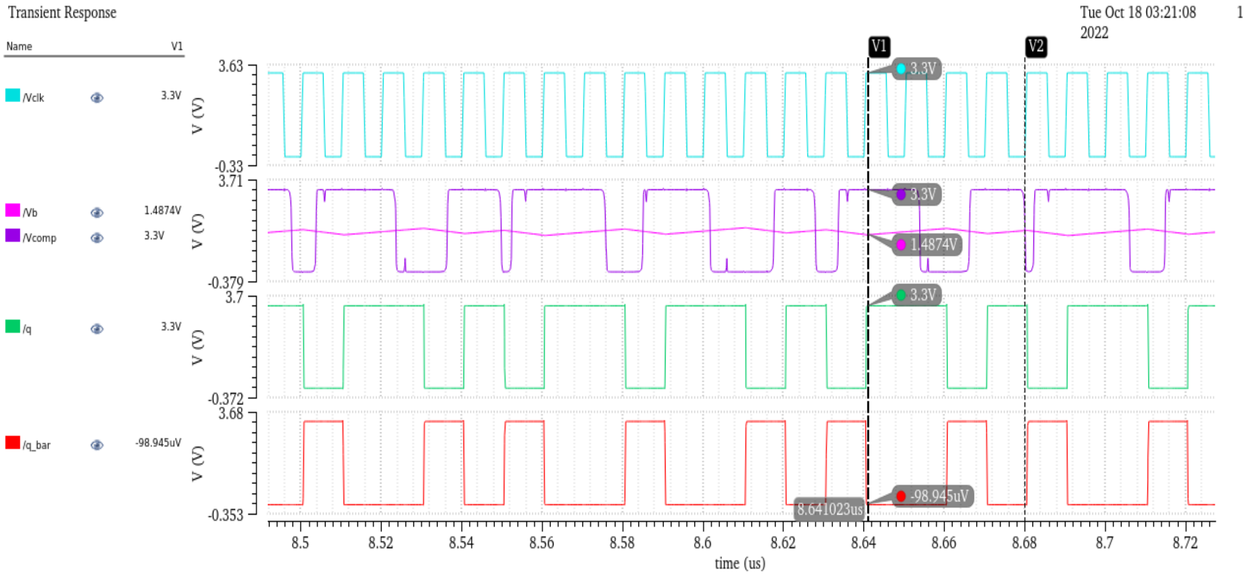

Figure 4.12 Simulation of the Circuit for 1st Method with Inverter ($I_{ref} > I_{in}$)

Several simulations are conducted for different values of $I_{in} < 50\mu A$ and $I_{ref} = 50\mu A$ i.e., $I_{ref} > I_{in}$ for 1024 and 2048 clock cycles where one clock period $T_s = 10ns$. Using the equation (3) we can calculate the value of I_{in}. We wrote a MATLAB code to plot a graph for the inaccuracy between the real value and the calculated value.

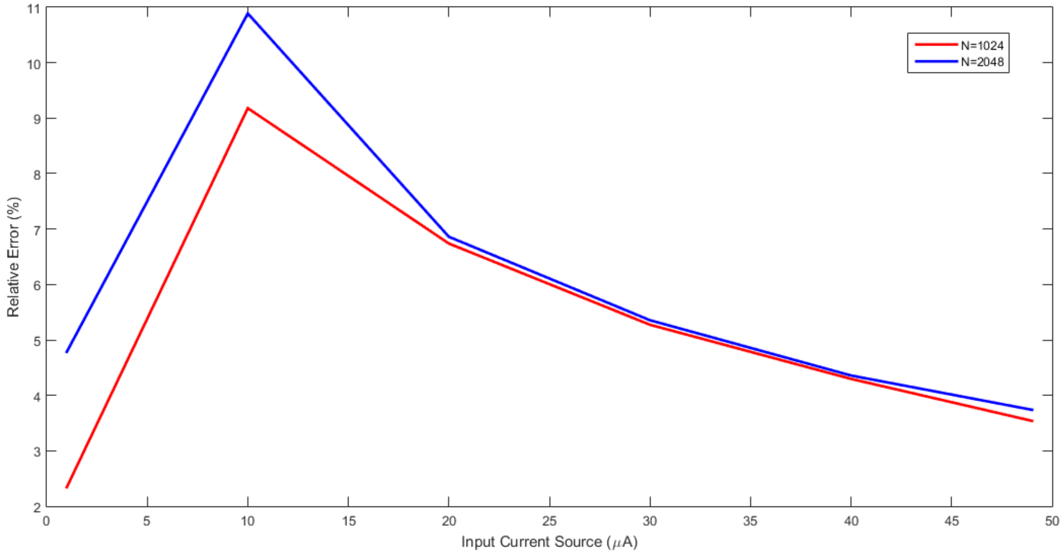

Figure 4.13 Relative Error vs Input Current Curve for 1st Method Implemented with Inverter

These curves do not follow the shape of the curves we found by analyzing the methodology. From the theoretical curve we can see that with increment of input current error increases. But, in simulation error is decreasing. Also, we estimated the maximum error in the theoretical investigation. From simulated result we can say that in real case the error can be minimized.

4.6 CIRCUIT IMPLEMENTATION OF PROPOSED METHOD 2 WITH INVERTER-BASED COMPARATOR

The circuit design of the second proposed method for the acquisition of power signature is shown in Figure 4.15. All the setup for this circuit is the same of the circuit setup for the second proposed implemented with comparator except instead of a comparator three series connected transistors are used.

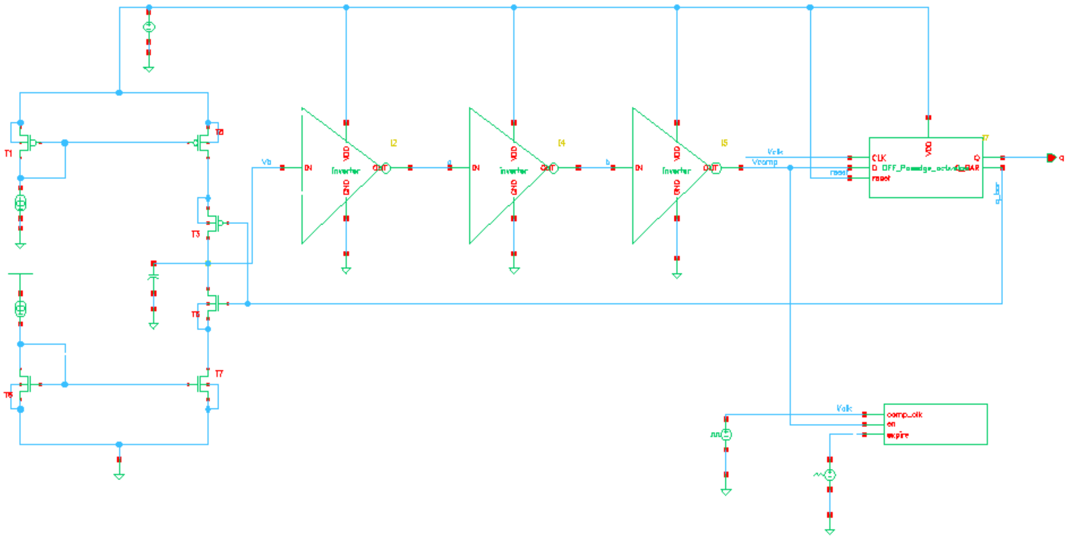

Figure 4.14 Circuit Implementation for 2nd Proposed Method with Inverter

The operation of this circuit can be explained as follows. When V_{comp} is low on the rising edge of clock cycle the outputs of the DFF, q and q_bar become low and high respectively. Now, q_bar is fed back to the T_3 and T_5 switches. As q_bar is high it turns off the transistor T_3 and turns on the transistor T_5. Hence, the capacitor, C attached to node b stops to be charged by I_{in} and starts to be discharged through I_{ref}. So, V_b starts to decrease and at time when it is below 1.6V at the end of the series of inverters the V_{comp} becomes high. This phenomenon makes the outputs of the DFF, q and q_bar high and low respectively at the next rising edge of the clock cycle. Now, q_bar is low it turns on the transistor T_3 and turns ff the transistor T_5. Hence, the capacitor, C attached to node b starts to be charged by I_{in} and stops to be discharged through I_{ref}. So, V_b starts to increase and at time when it is above the threshold voltage of the inverter, 1.65V at the end of the series of inverters the V_{comp} becomes high. The V_{comp} signal goes to the veriloga counter. The counter is enabled when the V_{comp} is low and counts the number of zero at the enable port for 1024 clock cycles. The simulation result for $I_{ref} = 50\mu A$ & $I_{in} = 20\mu A$ i.e., $I_{ref} > I_{in}$ is displayed in figure 4.5. For this condition the waveforms follow as the operation is stated.

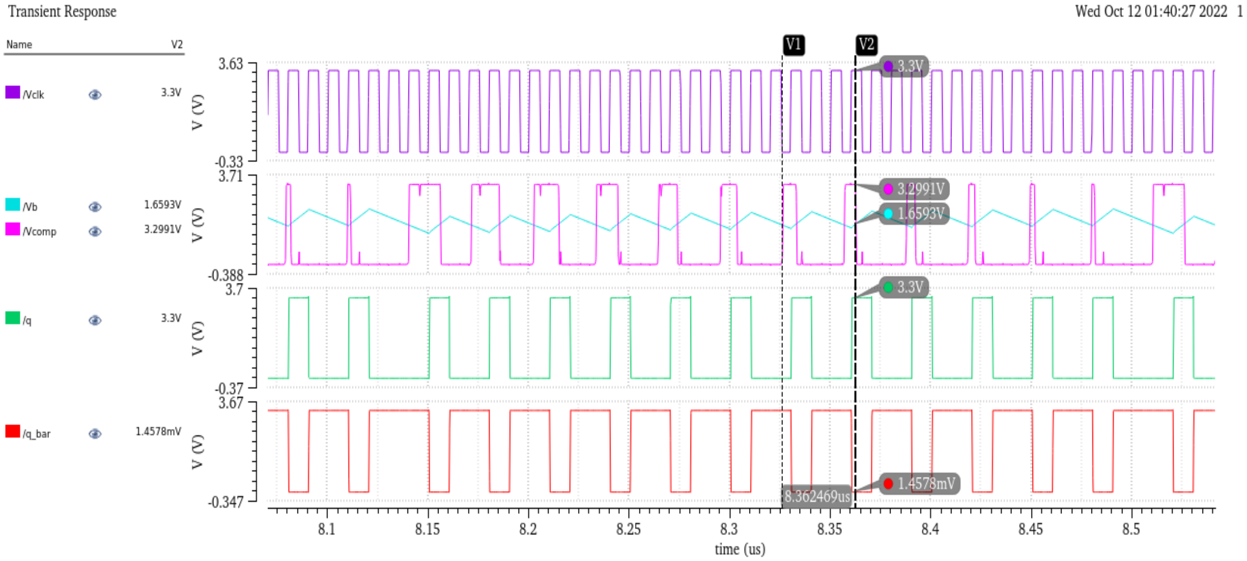

Figure 4.15 Simulation of the Circuit for 2nd Method with Inverter

Several simulations are conducted for different values of I_{in} for the range 1μA to 200μA and $I_{ref} = 50\mu A$ for 1024, 2048 and 4096 clock cycles where one clock period $T_s = 10ns$. Using the equation (10) we can calculate the value of I_{in}. We wrote a MATLAB code to plot a graph for the inaccuracy between the real value and the calculated value.

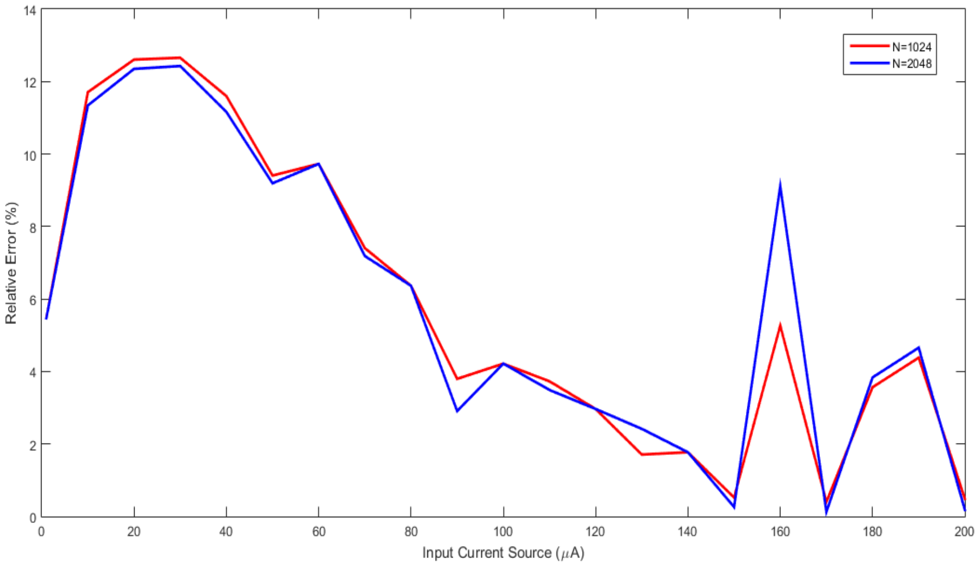

Figure 4.16 Relative Error vs Input Current Curve for 2nd Method Implemented with Inverter

We can compare the calculated values of the input current with the given source value to check the accuracy of different setups from table 1 and table 2. The calculated values are close to the given source value. If we analyze the data of the tables, we can see that when we are using larger number of total clock cycles the calculated input source value is closer to the given input source value for both circuits setups. Again, when the circuit is built with inverter the accuracy of the calculated value deteriorates. But, as exact value is not required, we can use the setup with inverter to collect power signatures because it gives reasonable value. Also, if we observe table 2 it is clear that after a certain range of input current source for a constant reference current source the circuit setup with latch-based comparator does not work properly whereas, the inverter-based comparator circuit gives quiet close calculated input current source value.

Table 1 Comparison Between Current Sources Being Monitored and the Calculated Current Values Found from Different Setups for the 1st Method

Input Current Source (µA)	N=1024		N=2048	
	Calculated Current with Comparator Setup (µA)	Calculated Current with Inverter Setup (µA)	Calculated Current with Comparator Setup (µA)	Calculated Current with Inverter Setup (µA)
1	1.02	0.97	1.00	0.95
10	9.81	9.08	9.79	8.91
20	19.43	18.65	19.45	18.62
30	29.10	28.41	29.12	28.39
40	38.81	38.28	38.84	38.25
49	47.50	47.26	47.48	47.16

Table 2 Comparison Between Current Sources Being Monitored and the Calculated Current Values Found from Different Setups for the 2nd Method

Input Current Source (µA)	N=1024		N=2048	
	Calculated Current with Comparator Setup (µA)	Calculated Current with Inverter Setup (µA)	Calculated Current with Comparator Setup (µA)	Calculated Current with Inverter Setup (µA)
1	1.04	0.94	1.02	0.94
10	10.59	11.17	10.52	11.17
20	20.81	22.52	20.86	22.52
30	30.88	33.79	30.88	33.79
40	40.94	44.63	40.94	44.63
50	50.58	54.70	50.58	54.70
60	60.34	65.83	60.58	65.83
70	70.18	75.18	70.04	75.18
80	79.62	85.09	79.62	85.09
90	90.27	93.41	90.08	93.41
100	100.14	104.21	99.92	104.21
110	108.51	114.10	108.26	114.10
120	117.86	123.55	118.14	123.55
130	124.74	127.77	125.04	127.77
140	134.83	142.48	134.50	142.48
150	141.76	150.78	141.76	150.78
160	150.78	151.57	150.39	151.57
170	150.78	170.68	150.39	170.68
180	150.78	173.58	150.39	173.58
190	150.78	181.67	150.39	181.67
200	150.78	200.98	150.39	200.98

Table 3 Statistics of Error for Proposed Method 1

Method	Number of Clock Cycle	Maximum Error	RMS Error	Avg relative Error
Implemented with Comparator	N=1024	1.49μA	0.88μA	2.69%
	N=2048	1.59 μA	0.88μA	2.29%
Implemented with Inverter	N=1024	49.21μA	16.03μA	5.22%
	N=2048	49.60 μA	16.20μA	5.99%

Table 4 Statistics of Error for Proposed Method 2

Method	Number of Clock Cycle	Maximum Error	RMS Error	Avg relative Error
Implemented with Comparator	N=1024	1.73μA	1.35μA	4.52%
	N=2048	1.83 μA	1.41μA	5.51%
Implemented with Inverter	N=1024	8.32μA	4.39μA	5.69%
	N=2048	14.58 μA	5.13μA	5.75%

From table 3 and table 4 we can state keeping every other factors same if we increase the number of clock cycle of operation for both setups for 1st method the error value decreases and for 2nd method the error value increases. On the other hand, for both method keeping other parameters constant, using comparator gives lower error than using an inverter. Using comparator in the circuit setup gives better performance. For having a simpler hardware design, we can use inverter circuits instead of a comparator though it can’t promise an accurate measurement. Yet if we observe the tables of the calculated current values, we can see that this circuit gives close output. As power signature analysis does not require an exact value, only a related value to circuit operation can provide with the desired contribution the circuit setup with inverter will work quite well.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 CONCLUSION

In this work, two methods for power signature generation are proposed which can be used in small IoT device surveillance. For both methods two different circuits are setup and were tested under different conditions to check the accuracy of the operation of the circuits. It shows that the power signature circuits could closely determine the value of source current, which is indicative of being able to detect changes caused by malicious attacks on an IoT device and has great potential on enhancing IoT security.

5.2 FUTURE WORK

In this work CMOS technology and simple, dependable designs were used to create a prototype digital circuitry. These circuits and simulations are mostly early findings that demonstrate that the suggested approach is effective in measuring power signatures and hold promise for further study and design. Investigating the causes of the lowering error value with an increase in the input current value when utilizing many inverters in a series may be done. Gain-boosted current mirrors or cascode structures can be designed to improve the current mirror circuit's ability to duplicate current values more accurately. To develop a layout for the implemented circuits and simulate the circuit using the netlist generated from the layout, small-scale, reliable circuits may be built. All outcomes in this study are based on the presumption that malicious assaults will change an IoT device's operational circumstances. A more detailed evaluation of its efficacy might be carried out by running system level simulation to show how to employ the designed circuits in IoT security applications.

REFERENCES

[1] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 336-341.

[2] Yong Ho Hwang, “IoT Security & Privacy: Threats and Challenges,” 1st ACM Workshop on IoT Privacy, Trust, and Security (IoTPTS '15), New York, NY, 2015.

[3] D. Millan, “IoT (Internet of Things),” *Medium*, Aug. 18, 2021. https://danielmillanalvarez.medium.com/iot-internet-of-things-d6b72c9a716b.

[4] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT Security:Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology,” *Internet of Things*, vol. 11, p. 100227, May 2020, doi: https://doi.org/10.1016/j.iot.2020.100227.

[5] W. Wang, Y. Yu, F. Standaert, J. Liu, Z. Guo and D. Gu, "Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 5, pp. 1301-1316, May 2018.

[6] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti and A. Trifiletti, "Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 61, no. 2, pp. 429-442, Feb. 2014.

[7] G. Dabosville, J. Doget and E. Prouff, "A New Second-Order Side Channel Attack Based on Linear Regression," in IEEE Transactions on Computers, vol. 62, no. 8, pp. 1629- 1640, Aug. 2013.

[8] “An In-Depth Dive Into Series vs. Parallel Circuits,” *resources.pcb.cadence.com*. https://resources.pcb.cadence.com/blog/an-in-depth-dive-into-series-vs-parallel-circuits (accessed Feb. 14, 2023)

[9] V. Prakash, A. V. Singh and S. Kumar Khatri, "A New Model of Light Weight Hybrid Cryptography for Internet of Things," 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2019, pp. 282-285.

[10] S. Roy, U. Rawat and J. Karjee, "A Lightweight Cellular Automata Based Encryption Technique for IoT Applications," in IEEE Access, vol. 7, pp. 39782-39793, 2019.

[11] Y. Shi, J. Han, X. Wang, J. Gao and H. Fan, "An Obfuscatable Aggregatable Signcryption Scheme for Unattended Devices in IoT Systems," in IEEE Internet of Things Journal, vol. 4, no. 4, pp. 1067-1081, Aug. 2017.

[12] S.A.Y. Hunn, S. Z. Naziri, N. Idris, “The development of tiny encryption algorithm (TEA) crypto-core for mobile systems”, 2012 IEEE International Conference on Electronic Design, Systems and Applications, IEEE, Kuala Lumpur, 2012, pp. 45-49.

[13] D. Virmani, N. Beniwal, G. Mandal, S. Talwar, “Enhanced Tiny Encryption Algorithm with Embedding”, International Journal of Computers and Technology, June 2013, vo. 7.

[14] Rajesh, Sreeja, et al. “A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices.” Symmetry (20738994), vol. 11, no. 2, Feb. 2019, p. 293.

[15] J. Lee, M. Kim, G. Shin and Y. Lee, "A 20F2 Area-Efficient Differential NAND-Structured Physically Unclonable Function for Low-Cost IoT Security," in IEEE Solid-State Circuits Letters, vol. 2, no. 9, pp. 139-142, Sept. 2019.

[16] J. Yoo, D. Kim, H. Park, M. Shim, C. Lee and C. Kim, "Physically Unclonable Function Using Ring Oscillator Collapse in 0.5 V Near-Threshold Voltage for Low-Power Internet of Things," 2018 IEEE International Conference on Consumer Electronics - Asia (ICCE-Asia), Jeju, 2018, pp. 206-212.

[17] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues and Y. Park, "Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions," in IEEE Access, vol. 7, pp. 85627-85644, 2019.

[18] V.R. Laguduva, S.A. Islam, S. Aakur, S. Katkoori, R. Karam. “Machine Learning based IoT Edge Node Security Attack and Countermeasures”, 2019 IEEE Computer Society Annual Symposium on VLSI, IEEE, Miami, FL, 17 September 2019, pp. 670-675.

[19] L. Bolotnyy, G. Robins. “Physically Unclonable Function-Based Security and Privacy in RFID Systems”, Annual IEEE International Conference on Pervasive Computing and Communications, IEEE, White Plains, NY, 19-23 March 2007, pp. 211-220.

[20] Oliver Kommerling and Fritz Kommerling, “Anti tamper encapsulation for an integrated circuit,” US Patent, US7005733B2, 2006

[21] D. Thompson and H. Wang, “Integrated Power Signature Generation Circuit for IoT Abnormality Detection,” *ACM Journal on Emerging Technologies in Computing Systems*, vol. 18, no. 1, pp. 1–13, Jan. 2022, doi: https://doi.org/10.1145/3460476.

[22] D. Thompson, “DESIGN OF EMBEDDED POWER SIGNATURE GENERATION CIRCUITS FOR INTERNET OF THINGS SECURITY,” *Theses*, May 2020, Available: https://opensiuc.lib.siu.edu/theses/2707/

[23] D. E. Thompson, M. Kamruzzaman Shuvo and H. Wang, "Digital LDO Based Power Signature Generation Circuit for IoT Security," *2020 IEEE 63rd International Midwest*

Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, 2020, pp. 1076-1079, doi: 10.1109/MWSCAS48704.2020.9184550.

[24] “What is IoT Security? - Definition from TechTarget.com,” *IoT Agenda*. https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security

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

[26] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[27] W. Wang, Y. Yu, F. Standaert, J. Liu, Z. Guo and D. Gu, "Ridge-Based DPA: Improvement of Differential Power Analysis For Nanoscale Chips," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 5, pp. 1301-1316, May 2018

[28] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti and A. Trifiletti, "Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 61, no. 2, pp. 429-442, Feb. 2014.

[29] G. Dabosville, J. Doget and E. Prouff, "A New Second-Order Side Channel Attack Based on Linear Regression," in IEEE Transactions on Computers, vol. 62, no. 8, pp. 1629-1640, Aug. 2013

[30] A. Jha, “IoT Security - Part 19 (101 - Introduction to Side Channel Attacks (SCA)),” *Payatu*, Dec. 08, 2020. https://payatu.com/blog/side-channel-attack-basics/ (accessed Feb. 18, 2023).

[31]a href="https://contest.techbriefs.com/account/profile/caguayog">Carlos Aguayo Gonzalez (caguayog), “Power Fingerprinting Monitor: Protecting Critical Infrastructure from Cyber Attack,” *Techbriefs.com*, Jul. 2013. https://contest.techbriefs.com/2013/entries/safety-and-security/3840 (accessed Dec. 06, 2019).

[32] C. R. A. Gonzalez, J. H. Reed. “Power fingerprinting in SDR integrity assessment for security and regulatory compliance”, Analog Integrated Circuits and Signal Processing, Springer US, 2011.

[33] Robert Bridges, Jarilyn Hernandez Jimenez, Jeffrey Nichols, Katerina Goseva-Popstojanova, Stacy Prowell, “Towards Malware Detection via CPU Power Consumption: Data Collection Design and Analytics (Extended Version),” arXiv:1805.06541v1 [cs.CR] 16 May 2018

[34] C. Hsu, "Application Power Signature Analysis," 2014 IEEE International Parallel & Distributed Processing Symposium Workshops, Phoenix, AZ, 2014, pp. 782-789

[35] K. Wu, H. Li, T. Chen, and F. Yu. 2009. Simple power analysis on elliptic curve cryptosystems and countermeasures:
Practical work. *2009 Second International Symposium on Electronic Commerce and Security, Nanchang* 2009, 21–24.

[36] S. Sun. 2008. Experiments in attacking FPGA-based embedded systems using differential power analysis. *IEEE Inter- national Conference on Electro/Information Technology, Ames, IA* 2008, 7–12.

[37] J. P. Hurst and A. D. Singh. 1997. A differential built-in current sensor design for high-speed IDDQ testing. In *IEEE Journal of Solid-State Circuits* 32, 1 (1997), 122–125
.

[38] I. Pecuh, M. Margala, and V. Stopjakova. 1999. 1.5 volts Iddq/Iddt current monitor. *Engineering Solutions for the Next Millennium. 1999 IEEE Canadian Conference on Electrical and Computer Engineering (Cat. No.99TH8411),* Edmonton, Alberta, Canada 1999, 472–476.

[39] Y. Cao, C. Chang, and S. Chen. 2014. A cluster-based distributed active current sensing circuit for hardware trojan detection. In *IEEE Transactions on Information Forensics and Security* 9, 12 (2014), 2220–2231.

[40] B. Shanyour and S. Tragoudas. 2018. Detection of low power trojans in standard cell designs using built-in current sensors. *2018 IEEE International Test Conference (ITC),* Phoenix, AZ, USA 2018, 1–10.

[41] C. Y. Leung, P. K. T. Mok, K. N. Leung, and M. Chan. 2005. An integrated CMOS current-sensing circuit for low-voltage
current-mode buck regulator. In *IEEE Transactions on Circuits and Systems II: Express Briefs* 52, 7 (2005), 394–397.

[42] "Offset Voltage - an overview | ScienceDirect Topics," *www.sciencedirect.com*. https://www.sciencedirect.com/topics/engineering/offset-voltage

[43] "Logic Levels - learn.sparkfun.com," *learn.sparkfun.com*. https://learn.sparkfun.com/tutorials/logic-levels/all

[44] "comparator gain vs channel lenth of transistor - Google Search," *www.google.com*. https://www.google.com/search?client=firefox-b-1-d&q=comparator+gain+vs+channel+lenth+of+transistor (accessed Feb. 12, 2023)

[45] "[SOLVED] - is length important in current mirrors?," *Forum for Electronics*. https://www.edaboard.com/threads/is-length-important-in-current-mirrors.272069/ (accessed Feb. 12, 2023

VITA

Graduate School
Southern Illinois University Carbondale

Arunima Aindrila Badhon

arunima.ece2k13@gmail.com

Khulna University of Engineering and Technology
Bachelor of Science, Electronics and Communication Engineering, March 2018

Thesis Paper Title:
A Current to Digital Converter for Power Signature Generation Applications

Major Professor: Dr. Haibo Wang

Publications:

R. Akter *et al.*, “Impact Analysis of Different Gap on CIGS Photovoltaic Device with MoSe2 as Tunnel Layer,” *Smart Technologies for Energy, Environment and Sustainable Development*, *Vol 1*, pp. 443–457, 2022, doi: https://doi.org/10.1007/978-981-16-6875-3_36