University of Kentucky

UKnowledge

2021

Combining Approximate Computing And Adiabatic Logic For Low-Power And Energy-Efficient Iot Edge Computing

Wu Yang

University of Kentucky, frelol2@outlook.com
Digital Object Identifier: https://doi.org/10.13023/etd.2021.259

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Recommended Citation

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.

<div align="right">

Wu Yang, Student

Dr. Himanshu Thapliyal, Major Professor

Dr. Daniel L. Lau, Director of Graduate Studies

</div>

COMBINING APPROXIMATE COMPUTING AND ADIABATIC LOGIC FOR
LOW-POWER AND ENERGY-EFFICIENT IOT EDGE COMPUTING

THESIS

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Electrical Engineering
in the College of Engineering
at the University of Kentucky

By
Wu Yang
Lexington, Kentucky
Director: Dr. Himanshu Thapliyal
Lexington, Kentucky
2021

ABSTRACT OF THESIS

COMBINING APPROXIMATE COMPUTING AND ADIABATIC LOGIC FOR
LOW-POWER AND ENERGY-EFFICIENT IOT EDGE COMPUTING

The growing data-intensive applications that run on IoT edge devices require the circuit to be low-power consumption and energy-efficient for limited resources. As conventional Complementary Metal-Oxide-Semiconductor (CMOS) scales down to the nanometer technology node, it reaches its limits, such as leakage and power consumption. Adiabatic logic and approximate computing are emerging techniques for the low-power circuit. Adiabatic logic can recycle energy which is a promising solution for building energy-efficient circuits. However, the power clock scheme and dual-rail structure of adiabatic logic increase the overall area. Power consumption is further reduced by applying approximate computing while reducing the complexity and size of the circuit.

Therefore, to investigate the benefits of approximate computing combined with adiabatic logic, we propose two adiabatic logic based approximate adders. The proposed approximate adders use the advantage of dual-rail logic to shrink the overall size and reduce energy consumption. The two proposed designs are True Sum Approximate Adder (TSAA) and True Carry-out Approximate Adder (TCAA). TSAA approximates the Carryout based on the accurate Sum, and TCAA approximates the Sum based on the precise Carryout.

We performed simulations using 45nm technology in Cadence Spectre. Comparing with CMOS based accurate mirror adder (AMA) at 100 MHz, a power-saving of 83.26% and energy saving of 66.54% in PFAL based TSAA (PFAL: Positive Feedback Adiabatic Logic) is achieved. Further, we achieved a power saving of 87.22% and an energy saving of 74.43% in PFAL based TCAA compared to CMOS based accurate mirror adder (AMA). It is illustrated that PFAL based TCAA consumes 24.0% less power and energy per cycle compared to PFAL based TSAA.

Further, we have proposed the True Sum Approximate Adder (TSAA) and the True Carry-out Approximate Adder (TCAA) that are energy-efficient and secured against DPA attacks. At 12.5 MHz operating frequency and 45 nm technology node, the DPA-resistant adiabatic TSAA and TCAA achieved power savings of 95.4% and

95.48%, energy savings of 90.80%, and 90.96% in comparison with the standard CMOS AMA.

Wu Yang

_____

July 22, 2021

_____

COMBINING APPROXIMATE COMPUTING AND ADIABATIC LOGIC FOR
LOW-POWER AND ENERGY-EFFICIENT IOT EDGE COMPUTING

By

Wu Yang

Dr. Himanshu Thapliyal

(Director of Thesis)

Dr. Daniel Lau

(Director of Graduate Studies)

July 22, 2021

(Date)

ACKNOWLEDGMENTS

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Internet of Things (IoT) is the connected device that exchanges data through a network for intelligent applications. IoT devices are highly integrated with our daily lives, such as smart homes, smart cities, and health care, which gives us the benefit of monitoring, predicting, and controlling the environment around us. Those devices includes sensors (optical, thermal and moisture, etc) for industry or home, wearable devices, smartphone, radio frequency identification (RFID) [4] [5] [6]. IoT devices collect data and sent it to the cloud for further process. However, the rapid growth of the IoT market puts more pressure on the network infrastructure as the data generated by numerous IoT edge devices. As a prediction, the number of IoT devices will exceed 28 billion by the year 2022, and 75.44 billion by 2025 [7] [8]. Therefore, there is a need to design a new paradigm for handling the tremendous amount of data produced by IoT edge devices.

Edge computing is the emerging computing paradigm in which the computation process occurs at the edge of the network (near or at the IoT edge devices). Edge computing nodes are situated near the end-user. Thus, they are less affected by network traffic and have low latency. This results in increased privacy as less sensitive data is sent to the cloud server [5] [9]. Therefore, these features allow researchers to

build machine learning and deep learning with edge computing [5] [10]. However, developing machines or deep learning at the edge will require increase computational capability of the IoT devices and lead to a rise of power dissipation. Furthermore, most IoT devices have limited computation and energy resources. Hence, an energy-efficient and low-power solution is needed for IoT devices.
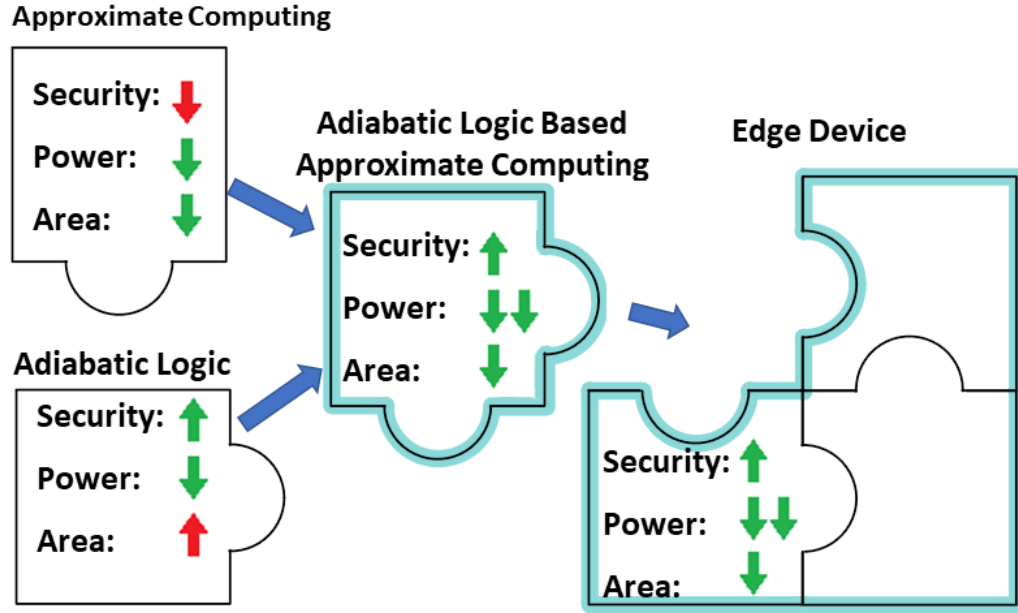
Figure 1.1: Combining the approximation computing and adiabatic logic (© 2021 IEEE.

The focus of this thesis is to explore the benefit of designing low-power and energy-efficient IoT devices with approximate computing combined with adiabatic logic, as illustrated in Fig.1.1. Approximate computing is suitable for building low-power circuits at the cost of inexact output, perfect for the error-tolerance application running on IoT edge devices. Additionally, approximate computing reduces the circuit complexity, which helps to reduce the overall size. Adiabatic logic is emerging for designing low-power and energy-efficient circuits but at the cost of the increased circuit size. Adiabatic logic recovers the charge in the load capacitors efficiently through the power clock and reuses those charges in the next clock cycle. Also, the correlation between data and power consumption which helps increase the resistance to the

Differential Power Analysis (DPA) attack when applying adiabatic logic [3].

1.1   Contribution of Thesis

This thesis presents a low-power and energy-efficient circuit with increased resistance to DPA attack by combining adiabatic logic and approximated computing. The contribution of this thesis can be summarized as follow:

1. True Sum based adiabatic approximate adder with reduced power and energy dissipation.

2. True Carry-out based adiabatic approximate adder with reduced power and energy dissipation.

3. Low-power and energy-efficient adiabatic approximate adders with increase resistance to DPA attack.

Two adiabatic logic-based approximate adders were proposed to illustrate the benefits of adiabatic logic combined with approximate computing. Simulation results indicated that adiabatic logic combined with approximate computing achieves low power, energy-efficient, and reduced areas with increased security against Differential Analysis attack (DPA).

1.2   Outline of Thesis

This thesis s organized as follows: Chapter 2 presents the background of adiabatic logic, approximate computing, and DPA attack. Chapter 3 introduces the adiabatic-based approximate adder. Then Chapter 4 explores the DPA resistance of adiabatic-based approximate adder. Next, Chapter 5 concludes the thesis.

The work presented in Chapter 3 and some portion of Chapter 1 and 2 were previously published in [11] "W. Yang and H. Thapliyal, Low-Power and Energy-Efficient Full Adders With Approximate Adiabatic Logic for Edge Computing," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) © 2020 IEEE". The work published in Chapter 4 and some portion of Chapter 1 and 2 were previously published in [12] "W. Yang and H. Thapliyal, Approximate Adiabatic Logic for Low-Power and Secure Edge Computing," in IEEE Consumer Electronics Magazine © 2021 IEEE".

Chapter 2

Background

This chapter will cover required background information needed to understand the successive chapters. The main focus will be on adiabatic logic, approximate computing and Differential Power Analysis (DPA) attack.

2.1 Approximate Computing

Approximate computing is a novel technology for designing low-power circuits with reduced accuracy as a trade-off. Inexact data leads the applications to fail or produce lower-quality outputs. However, most multimedia applications, such as audio, video, graphics, and wireless communications, have intrinsic tolerance to the inexact data. Additionally, the final outputs are interpreted by human senses which the slight difference of the quality is not noticeable. Therefore, the researcher utilized the feature to design the circuit with an acceptable error rate to reduce power dissipation [2].

In the range of acceptable quality, approximation computing reduces the power consumption with reduced quality output, as illustrated in Fig.2.1. Furthermore, approximate computing can be implemented in other stages: approximate systems, approximate software that can further reduce the effect of inexact data and enhance output quality.
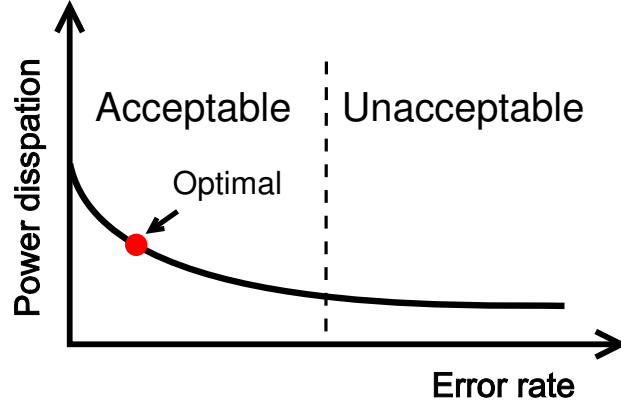
Figure 2.1: Power dissipation with respect to error rate

Conventional CMOS Mirror Adder (MA) is well known for its symmetrical property for equal fall time and rise time and inversion properties to reduce the critical path. The general schematic of MA has illustrated in Fig. 2.2. In [2], approximates are designed with approximated Carry-out (C_{out}) and approximated Sum (Sum) or just approximated Sum. Fig. 2.3 presents the approximation on the circuity of complementary output of the Carry-out ($\overline{C_{out}}$). The C_{out} circuitry is approximated by removing three transistors which results in 1 error output among 8 possible outputs. As a comparison, the approximated circuit has less power and reduced area than the accuracy circuit due to fewer transistors in the circuit. Additionally, power is further reduced as the decrease of switch activity [13].
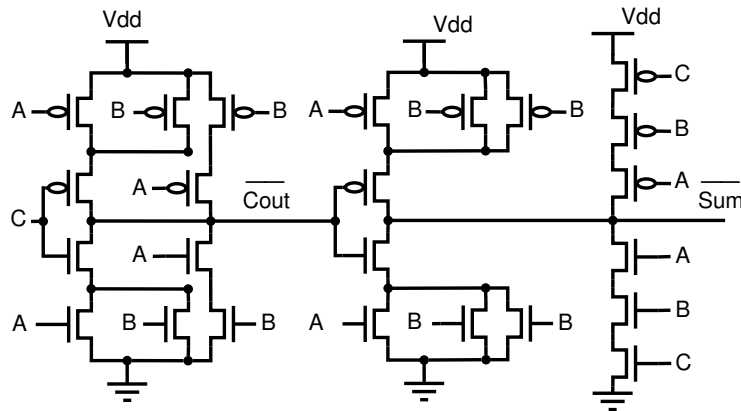
Figure 2.2: General Accurate Mirror Adder (AMA) schematic [1]

6
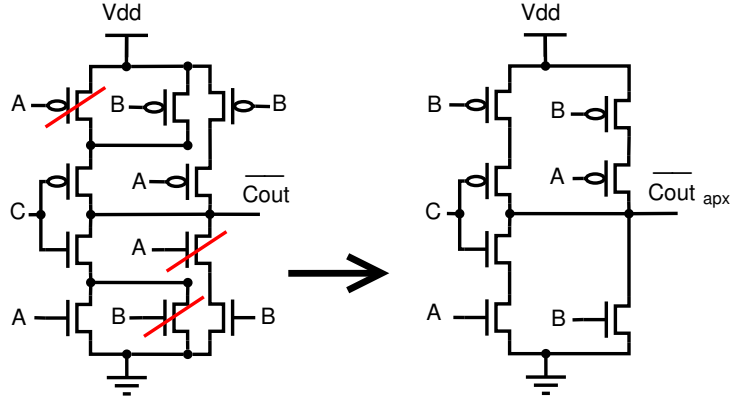
Figure 2.3: Approximated complementary output of Cout based on the mirror adder design [2]

2.2 Adiabatic Logic

Adiabatic logic is a promising low-power design technique to design low-power and energy-efficient circuits. Fig.2.4 shows the adiabatic charging/discharging of the load capacitor, where the F is the function block of the circuit, and $\overline{F}$ is the compliment function block of the circuit.
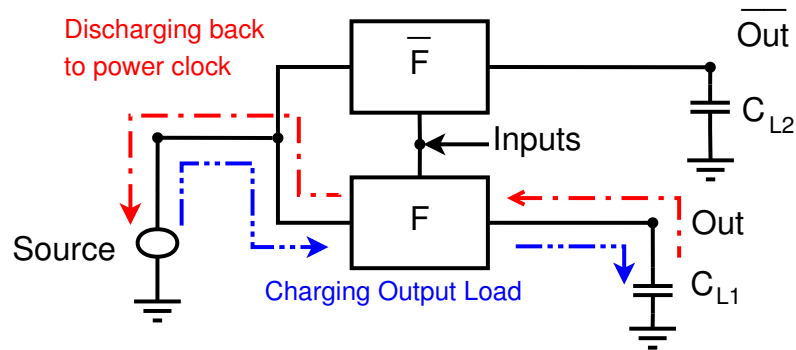
Figure 2.4: Operation of Adiabatic Logic

Adiabatic logic recycles the charges at load capacitance to the power clock instead of the GND, reducing the overall energy dissipation of the circuit. Additionally, the slow rising/falling clock can work as a constant current source, a primary requirement in adiabatic logic to minimize the loss due to the potential difference between source and drain. Therefore, the waveform of the power clock is in the form of trapezoidal,

triangular, or sinusoidal. Fig.2.5 shows the trapezoidal waveform, which is used in this thesis. The trapezoidal waveform has 4-phases which are waiting phase (W) stays at logic "0", evaluating phase (E) slowly ramp up to logic "1", the holding phase (H) remains at logic "1", and recovering phase (R) slowly ramp down to logic "0".
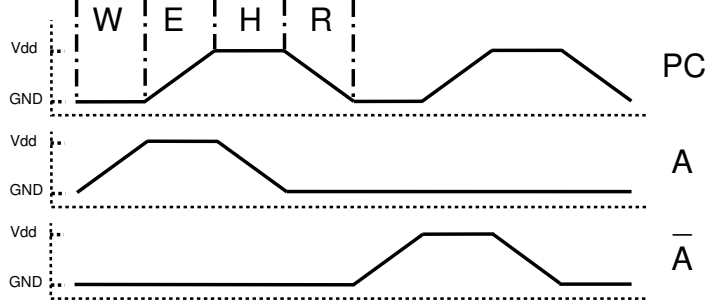
Figure 2.5: Trapezoidal waveform of power clock (PC) and dual inputs

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

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

Where V_{dd} is the full swing of the power clock, R is the parasitic resistance of the transistor, C is the load capacitance, and T is the transition period for charging/discharging time of the capacitor [14]. The energy loss in conventional CMOS is given by $E_{CMOS} = \frac{1}{2}CV_{dd}^2$, it's possible for the adiabatic logic has less energy dissipation than the conventional CMOS circuit when $T >> 2RC$ (refer to equation 2.1). Hence, the operational frequency of adiabatic logic should be restricted to kHz to a few MHz to minimize the energy loss. Additionally, the designer should minimize all the energy losses, such as adiabatic loss, non-adiabatic loss, and leakage, for designing an energy-efficient circuit [15] [16].

2.2.1 Adiabatic loss

The switch model of adiabatic loss is illustrated in Fig.2.6(a). Adiabatic loss occurs when charging and discharging the load capacitance through the PMOS transistor that is turned ON. Hence, the adiabatic loss is shown by,

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

Where V_{dd} is the full swing of the power clock, R_{on} is the ON-resistance of the channel, and C_L is the load capacitance, T is the transition period. From equation 2.2, the adiabatic loss can be minimized when choosing proper technology node and operational frequency [17] [16].
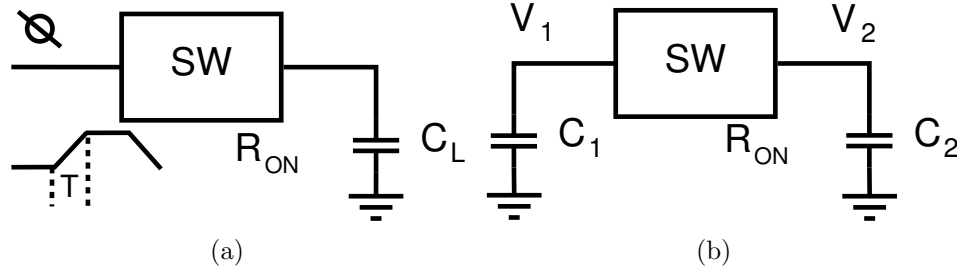
Figure 2.6: Switch model for illustrating the energy losses (a) adiabatic loss (b) non-adiabatic loss

2.2.2 Non-adiabatic loss

The switch model of non-adiabatic loss is illustrated in Fig.2.6(b). Non-adiabatic occurs when the voltage difference between two nodes of the switch is not neglectable ($|V_{1-2}| \not\approx 0V$). The Non-adiabatic loss is given by,

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

Where V_1 and V_2 are the voltages at the two nodes just before the switch is turned on, and C_1 and C_2 are the capacitance of the two nodes connected to the switch.

9

From equation 2.3, the adiabatic loss is independent of the operational frequency. Therefore, the non-adiabatic loss is much higher than adiabatic loss when the circuit operates at low-frequency [17]. Additionally, the power clock needs to slowly rise to logic "1" and fall to logic "0" for reducing the potential difference between source and drain ($V_{ds} \approx 0V$) of the PMOS transistor. Therefore, the non-adiabatic loss can be eliminated if the transistor is turned ON when there is no potential difference between the two nodes.
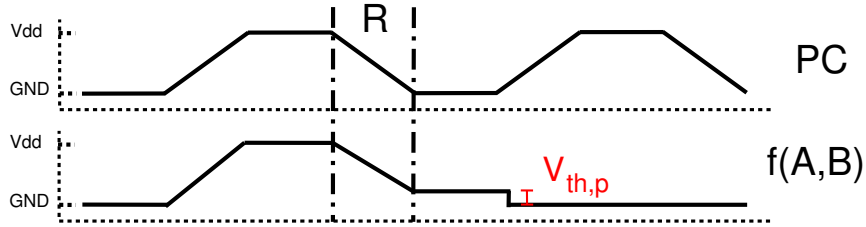
Figure 2.7: Residual charges at the output node

However, the output node can only be discharged to the threshold voltage (V_{th_p}) of the PMOS transistor, leading to a residual voltage at the output node, which is illustrated as Fig.2.7. Since the PMOS is turned OFF when the voltage of the power clock is less than the threshold voltage of the PMOS during discharging phase, the output node can't be fully discharged. Therefore, the residual charge leads to a potential difference between the two nodes. Hence, the equation 2.4 describes the energy loss due to the residual charge at the output node, where C is the capacitance [16] [15].

$$E_{non-adiabatic} = \frac{1}{2}CV_{th_p}^2 \tag{2.4}$$

2.2.3 Adiabatic leakage loss

As the CMOS technology reduces to sub-nano technology nodes, the energy loss due to leakage is not negligible and becomes one of the significant sources of energy
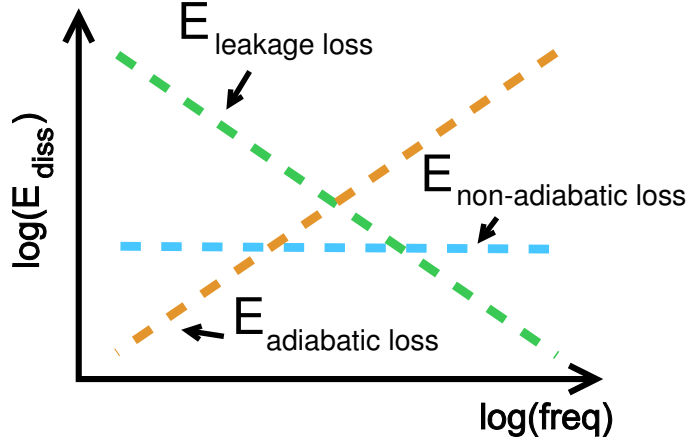
Figure 2.8: Loss mechanisms in adiabatic logic

dissipation. The current flows from the voltage supply to the ground during each evaluating phase in adiabatic logic. Additionally, leakage current leads to energy loss, and those energies cannot be recovered during the recovering phase. Therefore, the energy loss due to leakage current is proportional to the leakage current and operational frequency. The energy dissipation due to leakage is given by [15],

$$E_{leak} = V_{dd} \cdot \overline{I_{leak}} \frac{1}{f} \tag{2.5}$$

Where V_{DD} is the full swing of the voltage supply, f is the frequency of operation, and I_{leak} is the leakage current. From equation 2.5, the energy dissipation due to leakage current can be reduced by increasing the operating frequency. However, the $E_{adaibatic}$ is a positive proportion to the frequency, which leads to increased energy dissipation. Hence, frequency of operation is the key to energy loss in the adiabatic circuit. Fig.2.8 shows the three-loss mechanisms with respect to frequency, and the adiabatic circuit can be made energy-efficient by selecting proper operational frequency.

2.3 Correlation Power Analysis Attack

Side-channel attacks can reveal the secret key based on the information obtained from the cryptographic hardware. Side-channel attacks include power attacks, timing attacks, and electromagnetic attacks, etc. Further, the power analysis attack can be classified as Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA). SPA: an attacker directly observes a device's power consumption to determine the key of the cryptographic algorithm being used. DPA: a type of side-channel attack that can reveal a cryptographic device's secret key by statistically analyzing the correlation between the processed data and the power traces. CPA: the enhancement of DPA, which derives the correct key by using the correlation coefficient of statistics between the power traces and the values of the intermediate result of the key guess. These attacks are used in conjunction with hypothetical power models to reveal the secret key [18] [19] [20].

2.3.1 Differential Power Analysis Process

DPA attack finds the correlation between power dissipation and input plain text by measuring the power consumption while the cryptographic device performs the encryption. As the device computes the ciphertext, the power dissipation varies based on the change of state of the CMOS transistor, reflecting the circuit calculation. The power dissipation can be measured with a proper device, such as a digital sampling oscilloscope. Finally, the secret key can be revealed using statistical methods with those power traces and uniform plain texts. Substitution box (S-box) is an essential component of symmetric key algorithms commonly used in data encryption standard (DES) algorithm and advanced encryption standard algorithm (AES). Hence, the DPA attack on an S-box is used as a model to illustrate the DPA attack's main steps. DPA attack process is explained briefly as follows:

1. Adversary prepares expected intermediate output I with a set of plain text P and a set of hypothesis key Q. Let P_i represents the ith element in the set of plain text P and Q_k represents the kth element in the set of hypothesis key Q. The plain text is XORed secret key during each run of encryption, then pass to S-box to generate the intermediate output. Hence, the expected intermediate output I is compute with equation 2.6.

$$I_{n(i,k)} = SBox(P_{i,n} \oplus K_{k,n}) \tag{2.6}$$

   Where the S-box performs substitution algorithm $(SBox(x,y))$ on the XORed value, the n denotes the nth byte of P or Q [21].

2. Adversary measures the power consumption for each run with proper equipment like an oscilloscope. To obtain the current trace, the adversary measures the voltage across the resistor, placed in a series of the device's ground lines. The captured current trace is further sampled $M_{i,t}$ and corresponds to a particle input plain text P_i, where t denotes the tth element of the samples [21]. This current trace is presented by M matrix as illustrated in Fig.2.9.

3. After collecting data from the targeted device, a power model is created with the measured current traces. The power model keeps track of the transitions for each current trace. The transitions are categorized into two sets based on the power consumption. The "0" to "1" and "1" to "0" transitions are in the set of higher power dissipation, and "0" to "0" and "1" to "1" transitions are in the set of lower power dissipation. In general, hamming distance model is used for the power model. This model is illustrated by H matrix as shown in Fig.2.9.

4. For finding the correct key, each column of current traces M matrix is compared

13
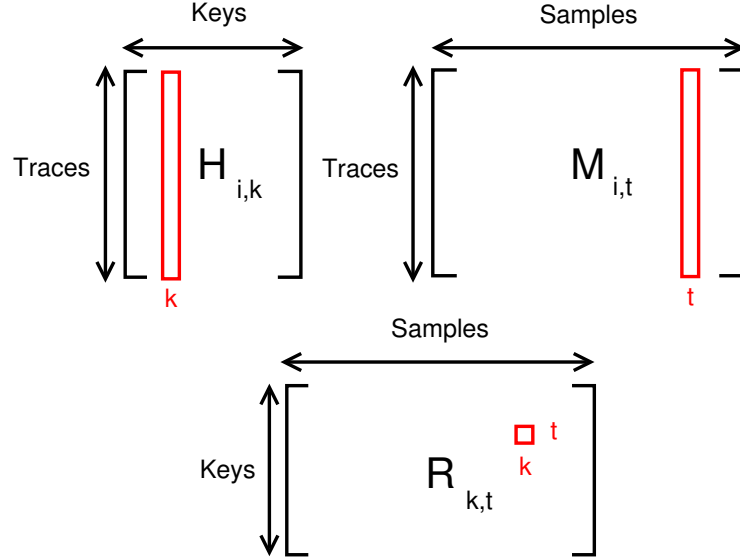
Figure 2.9: Correlation Matrix

with each column power consumption model H. Each column of M matrix represents the power consumption of a hypothesis key, and each column of H matrix represents the value of the current trace at a specific time. The correlation equation for find n correct key is given by equation 2.7.

$$r_{k,t} = \frac{\sum_{c=1}^{C}(h_{c,k} - \overline{h_k}) \cdot (m_{c,t} - \overline{m_t})}{\sqrt{\sum_{c=1}^{C}(h_{c,k} - \overline{h_k})^2 \cdot \sum_{c=1}^{C}(m_{c,t} - \overline{m_t})^2}} \qquad (2.7)$$

Where $\overline{h_i}$ and $\overline{m_i}$ denotes the average values of the columns of h_i and m_j respectively, C is the total number of record current traces. After performing a correlation calculation, the entry with maximal value in the correlation matrix R indicates the correct key, as illustrated in Fig.2.9.

Chapter 3

Approximate Adder With Adiabatic Logic

Adiabatic logic families are promising for designing energy-efficient circuits at the cost of an increase in area. Most adiabatic logic families, like Postie Feedback Adiabatic Logic (PFAL), are dual-rail in nature, which suffers doubling the size compared to conventional CMOS design. PFAL based full adder has 34 transistors in total, which has 10 more transistors compared to the Conventional COMS Mirror Adder (CMOS MA) (From Table 3.6). Additionally, Adiabatic logic needs extra buffers to ensure the circuit function correctly, as presented in Fig.3.1.
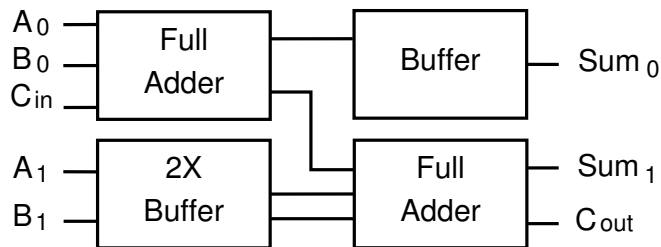
Figure 3.1: 2-bits ripple carry adder

When applying adiabatic logic, the circuit area is nearly double compared to the traditional CMOS design. Therefore, we could apply approximate computing to simplify the circuit and reduce the drawback of doubling the size when applying

adiabatic logic. Additionally, the proposed design illustrated that using approximate computing with adiabatic logic can produce low-power, energy-efficient, and reduced area circuits.

Material from this chapter was previously published in [12] as "W. Yang and H. Thapliyal, Low-Power and Energy-Efficient Full Adders With Approximate Adiabatic Logic for Edge Computing," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) © 2020 IEEE".

3.1   PFAL based Approximate Adder

We observe that the dual-rail property of the adiabatic logic can be used for approximating the sum or the carry-out output in the full adder to design low-power energy-efficient circuits with a reduced number of transistors.
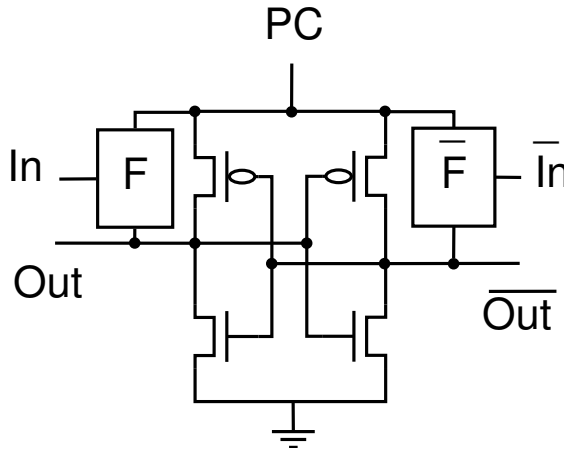
Figure 3.2: General schematic of PFAL (© 2020 IEEE).

Fig.3.2 shows the general schematic of PFAL, where block F and block $\overline{F}$ are the function blocks that generate the *Output* and $\overline{Output}$, respectively [15]. By applying the approximation to the PFAL circuit to approximate the output $\overline{F_1(x,y)}$ based on the complementary of the other output $F_2(x,y)$. Further, the full adder is the fundamental component of the digital signal processor, which is the backbone of many

multimedia applications. Therefore, we can design full adders use the complement output to approximate Sum or Carry-out output to shrink the overall size and reduce power and energy consumption. We can develop 1-bit approximate adiabatic logic adder as True Sum Approximate Adder (TSAA) based on equation (3.1) and True Carry-out Approximate Adder (TCAA) based on equation (3.2) to explore the combined benefit. TSAA is approximating the C_{out} based on the accurate Sum, and similarly, TCAA is approximating the Sum based on the accurate C_{out}.

$$
\begin{aligned}
F &= Sum \\
\overline{F} &= \overline{Sum} = Cout
\end{aligned}
\tag{3.1}
$$

$$
\begin{aligned}
F &= Cout \\
\overline{F} &= \overline{Cout} = Sum
\end{aligned}
\tag{3.2}
$$

3.1.1 True Sum Based Adder

The proposed True Sum Approximate Adder (TSAA) is implemented in Positive Feedback Adiabatic Logic (PFAL). The PFAL based schematic of TSAA is shown in Fig 3.3. The Table 3.1 shows the truth table of the TSAA, the $Cout$ is the complement of the Sum with only 2 different outputs, which occurred when both inputs are at logic 0 or logic 1 [2]. Utilizing the dual-rail property of the adiabatic logic, we can assign the $Cout_{TSAA}$ with the output of $\overline{Sum_{TSAA}}$ which gives us equation 3.3. Therefore, by the novel use of dual-rail logic in adiabatic circuits, we have eliminated the need for a separate circuit to compute $Cout$ and $\overline{Cout}$.

$$
\begin{aligned}
Sum_{TSAA} &= A \oplus B \oplus C \\
Cout_{TSAA} &= \overline{Sum_{TSAA}}
\end{aligned}
\tag{3.3}
$$
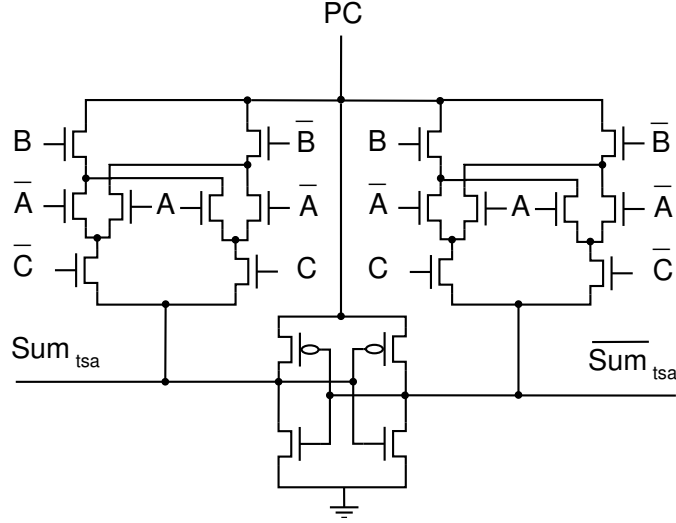
Figure 3.3: True Sum Approximate Adder Designed With PFAL (© 2020 IEEE).

Table 3.1: Truth table for Approximate Adders (difference between accurate outputs and approximate outputs are circled) (© 2020 IEEE)

Inputs			Accurate		TSAA		TCAA	
X	Y	Z	Sum	$Cout$	Sum	$Cout$	Sum	$Cout$
0	0	0	0	0	0	①	①	0
0	0	1	1	0	1	0	1	0
0	1	0	1	0	1	0	1	0
0	1	1	0	1	0	1	0	1
1	0	0	1	0	1	0	1	0
1	0	1	0	1	0	1	0	1
1	1	0	0	1	0	1	0	1
1	1	1	1	1	1	⓪	⓪	1

3.1.2   True Carry-Out Approximate Adder (TCAA)

The schematic of the proposed True Carry-out Approximate Adder (TCAA) is shown in Fig 3.4. The TCAA generates the correct Cout instead of Sum, and therefore the Sum_{TSAA} is assigned as $\overline{Cout_{TCAA}}$. The boolean equation of $Cout_{TCAA}$ is derived from Table 3.1 and is shown in equation 3.4. As the Sum_{TSAA} is assigned as the $\overline{Cout_{TCAA}}$, it removes the need for a separate PFAL block to generate the Sum output. Thus, the proposed circuit optimizes the power consumption and the area (number of transistors).

18

$$Cout_{TCAA} = B \cdot C + A \cdot C + A \cdot B$$

$$Sum_{TCAA} = \overline{Cout_{TCAA}}$$

(3.4)
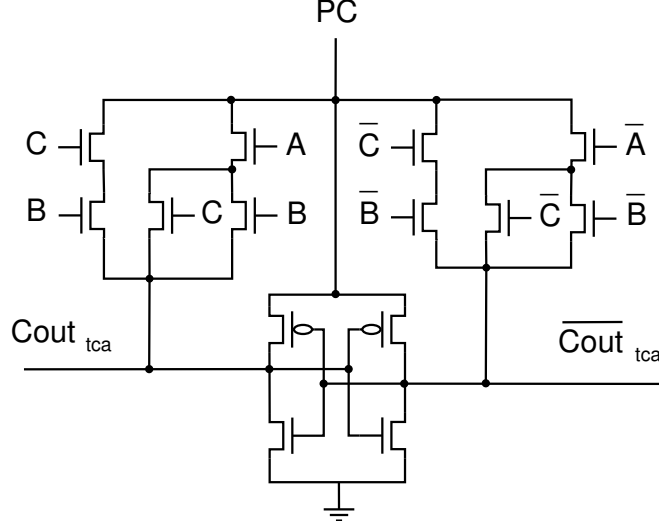
Figure 3.4: True Carryout Approximate Adder Designed With PFAL (© 2020 IEEE).

3.2 Simulation Results and Discussion

In this paper, PFAL based TSAA, PFAL based TCAA, CMOS based AMA [1], and CMOS based approximate mirror adders [2] are used for comparison. We have studied the proposed designs and compared them with the CMOS based accurate and approximate adder by frequency sweep from 1 MHz to 100 MHz. In addition, we performed simulations using 45nm technology in Cadence Spectre. Table 3.2 and Table 3.3 present the power consumption and energy consumption, respectively, at 10 fF by varying the frequency. The PFAL based TSAA has a lower power and energy consumption compared to the standard CMOS based AMA [1] and the four CMOS based approximate mirror adders proposed in [2] (CMOS $Apx1$, CMOS $Apx2$, CMOS $Apx3$ and CMOS $Apx4$). At 100 MHz, the PFAL based TSAA achieves power

and energy savings of 83.26% and 66.54%, respectively, compared to standard CMOS based AMA.

The PFAL based TCAA has the lowest power and energy consumption and obtains more power-saving and energy saving compared to standard CMOS based AMA and the four CMOS based approximate mirror adders proposed in [2](CMOS $Apx1$, CMOS $Apx2$, CMOS $Apx3$ and CMOS $Apx4$). Compared to the CMOS based AMA, the PFAL based TCAA yields power and energy savings of 87.22% and 74.43%, respectively, at 100 MHz. Further, from Tables 3.2 and 3.3, we conclude that the PFAL based TCAA obtains more power and energy savings than the PFAL based TSAA. At 100 MHz, the PFLA based TCAA has 23.63% less power consumption and 23.59% less energy consumption than the PFAL based TSAA.

Table 3.2: Power Consumption (nW) of PFAL based TSAA and CMOS based adders at different frequencies (© 2020 IEEE).

	1 MHz	10 MHz	50 MHz	100 MHz
CMOS AMA [1]	25.46	222.1	786.8	1492
CMOS $Apx1$ [2]	17.98	163.6	560.0	978.4
CMOS $Apx2$ [2]	17.13	166.0	760.2	1289
CMOS $Apx3$ [2]	11.39	111.3	557.9	1116
CMOS $Apx4$ [2]	15.12	139.7	591.4	1142
Proposed PFAL TSAA	0.073	3.6	71.72	249.7
Proposed PFAL TCAA	0.043	2.589	54.10	190.7

Table 3.3: Energy Consumption (fJ) of PFAL based TSAA and CMOS based adders at different frequencies (© 2020 IEEE).

	1 MHz	10 MHz	50 MHz	100 MHz
CMOS AMA [1]	101.8	88.83	62.94	59.68
CMOS $Apx1$ [2]	71.93	65.43	44.8	39.13
CMOS $Apx2$ [2]	68.52	66.4	60.82	51.54
CMOS $Apx3$ [2]	45.56	44.52	44.64	44.66
CMOS $Apx4$ [2]	60.46	55.89	47.32	45.68
Proposed PFAL TSAA	0.585	2.88	11.48	19.97
Proposed PFAL TCAA	0.347	2.072	8.656	15.26

3.2.1 TSAA and TCAA with Different Load Capacitance

To evaluate the drive strengths of the proposed adiabatic approximate adders, we have performed more simulations by varying the load capacitance at 100MHz. Fig. 3.5 and Fig. 3.6 show that PFAL based TCAA obtains more power and energy savings than PFAL based TSAA. Further, PFAL based TCAA and PFAL based TSAA are less sensitive to the change of load capacitance compared to the CMOS AMA. Table 3.4 and Table 3.5 present the comparison results of the PFAL based TSAA and TCAA in terms of power dissipation and energy dissipation per cycle.

At 20fF load capacitance, the power consumption of PFAL based TSAA is 817.5nW, and the power consumption of PFAL based TCAA is 620.7nW. Further, the energy per cycle consumption of PFAL based TSAA is 65.4fJ, and the energy per cycle consumption of PFAL based TSAA PFAL based TCAA is 49.66fJ. Additionally, PFAL based TCAA consumes 24.0% less power and energy per cycle compared to PFAL based TSAA. However, the proposed designs have a higher decline rate in energy savings compared to power saving.

Table 3.4: Power Consumption (nW) of CMOS AMA, PFAL based TSAA and PFAL based TCAA with different load capacitance (© 2020 IEEE).

	0fF	5fF	10fF	15fF	20fF
CMOS AMA [1]	220.1	866.2	1492	2119	2745
Proposed PFAL TSAA	8.454	84.28	249.7	498.6	817.5
Proposed PFAL TCAA	5.368	62.87	190.7	387.1	620.7

Table 3.5: Energy Per Cycle (fJ/Cycle) of CMOS AMA, PFAL based TSAA and PFAL based TCAA with different capacitance loads (© 2020 IEEE).

	0fF	5fF	10fF	15fF	20fF
CMOS AMA [1]	8.804	34.65	59.68	84.75	109.8
Proposed PFAL TSAA	0.6763	6.743	19.97	39.89	65.4
Proposed PFAL TCAA	0.4294	5.029	15.26	30.25	49.66
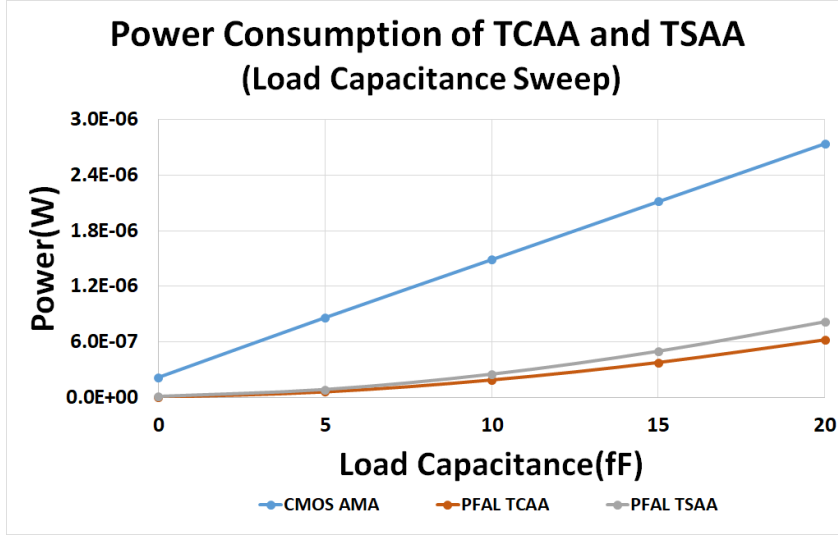
Figure 3.5: Power Consumption (W) of PFAL based TSAA, PFAL based TCAA and CMOS AMA (© 2020 IEEE)
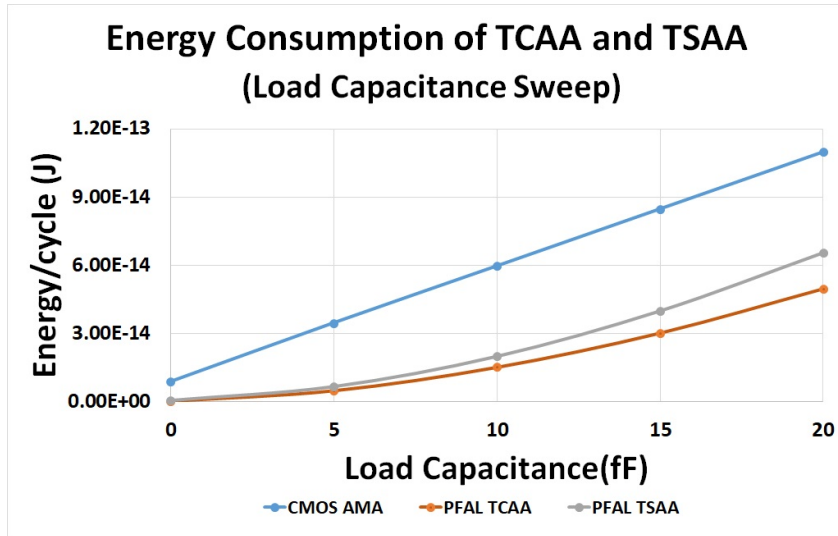
Figure 3.6: Energy Consumption (J/Cycle) of PFAL based TSAA, PFAL based TCAA and CMOS AMA (© 2020 IEEE).

3.2.2   Transistor Count

Table 3.6 shows the transistor count of the conventional CMOS based accurate mirror adder (AMA) [1], CMOS based approximate mirror adders [2], and PFAL based TSAA and TCAA. From Table 3.6, PFAL based TSAA has fewer transistors than the CMOS based AMA and PFAL based TCAA has nearly 50% fewer transistors

compared to the CMOS based AMA.

Table 3.6: Transistors Count in TSAA, TCAA and CMOS Based Adders (© 2020 IEEE).

	PMOS	NMOS	Total
CMOS AMA [1]	12	12	24
CMOS$apx1$ [2]	8	8	16
CMOS$apx2$ [2]	7	7	14
CMOS$apx3$ [2]	6	5	11
CMOS$apx4$ [2]	5	6	11
Proposed PFAL TSAA	2	18	20
Proposed PFAL TCAA	2	12	14

3.3   Summary

In this chapter, we have investigated and demonstrated that the combination of adiabatic logic and approximate computing could produce low-power design solutions for edge computing. Two novel adiabatic approximate adders are proposed using the novel application of the dual-rail property of adiabatic logic. The results show a significant decrease in power and energy consumption in the adiabatic logic based approximate adders compared to the conventional CMOS design. Furthermore, proposed designs are less sensitive to the load capacitance when compared to the traditional CMOS adder. Finally, the approximation on the dual-rail property allows the proposed designs to have less device count (number of the transistor) compared to the conventional CMOS and reduce the drawback of doubling the area when applying adiabatic logic. Thus, it is concluded that the proposed adiabatic True Carry-out Approximate Adder (TCAA) is better than the proposed adiabatic True Sum Approximate Adder (TSAA) in terms of area, power, and energy consumption.

Chapter 4

Approximate Adiabatic Adder with enhance security

Approximate computing is promising for error-tolerant apps that run on IoT edge devices. However, the cybersecurity solutions are not yet fully addressed [22,23]. For example, in [22], the author pointed out that an approximate adder has a positive correlation between output and power consumption, which increases as the error rate increases. Additionally, Adversaries could launch several attacks on the approximate circuits, such as side-channel attack and reverse engineering [23,24].

Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) is one of the adiabatic logic that is secured against side-channel attack [3]. Therefore, the hardware will have increased security by applying EE-SPFAL. In this chapter, we will demonstrate that by using approximate computation with adiabatic logic, it is possible to generate energy-efficient, low-power, and reduced area circuits with enhanced security (Figure 1.1). Furthermore, the benefits will illustrate with the case study of a full adder that the approximation computing can provide resistance against side-channel attacks such as Differential Power Analysis (DPA) attacks when implemented with adiabatic logic.

Material from this chapter was previously published in [12] "W. Yang and H. Thapliyal, Approximate Adiabatic Logic for Low-Power and Secure Edge Computing," in IEEE Consumer Electronics Magazine © 2021 IEEE".

4.1   EE-SPFAL based Approximate Adders

Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) [3] is an adiabatic logic family which is suitable to design low-power and secured adiabatic circuit. EE-SPFAL has uniform power consumption and is secure against Differential Power Analysis (DPA) based attacks. A general schematic of EE-SPFAL is shown in Fig.4.1, the block F and block $\overline{F}$ generate the $Output$ and $\overline{Output}$, respectively. Therefore, to minimize the total size and decrease power and energy consumption, the two proposed adders use the complementary output to approximate Sum or Carry-out outputs. Hence, the two approximate adders namely the True Sum Approximate Adder (TSAA) based on equation 3.1 and True Carry-out Approximate Adder (TCAA) based on equation 3.2 are developed.
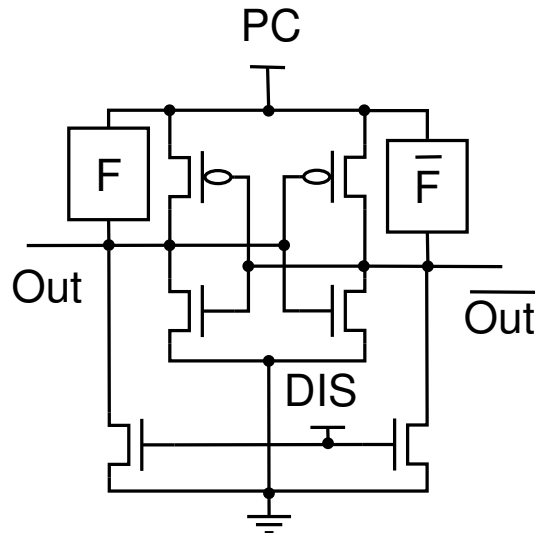
Figure 4.1: General schematic of EE-SPFAL [3] (© 2021 IEEE).

4.1.1 True Sum Approximate Adder (TSAA)

The schematic of TSAA based on EE-SPFAL is shown in Fig.4.2 where $Cout$ is the Sum complement. We have used the dual-rail property of the adiabatic logic to develop $Cout$ as the complement of the Sum (Equation 4.1). We, therefore, removed the need for a separate circuit to compute $Cout$ and $\overline{Cout}$.

$$Sum_{TSAA} = A \oplus B \oplus C$$
$$Cout_{TSAA} = \overline{Sum_{TSAA}}$$

(4.1)
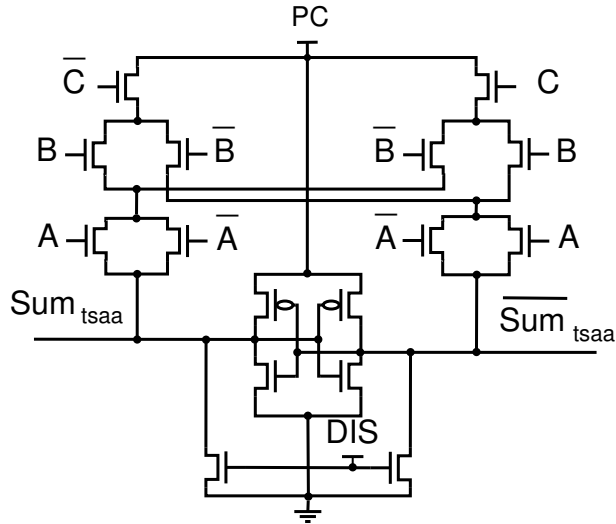
Figure 4.2: EE-SPFAL based True Sum Approximate Adder (© 2021 IEEE).

4.1.2 True Carry-Out Approximate Adder (TCAA)

The schematic of TCAA based on EE-SPFAL is shown in Fig.4.3. In TCAA, the Sum_{TSAA} is computed as $\overline{Cout_{TCAA}}$ (Equation 4.2). We, therefore, removed the need for a separate circuit to generate the Sum output.

$$Cout_{TCAA} = B \cdot C + A \cdot C + A \cdot B$$

$$Sum_{TCAA} = \overline{Cout_{TCAA}}$$

(4.2)
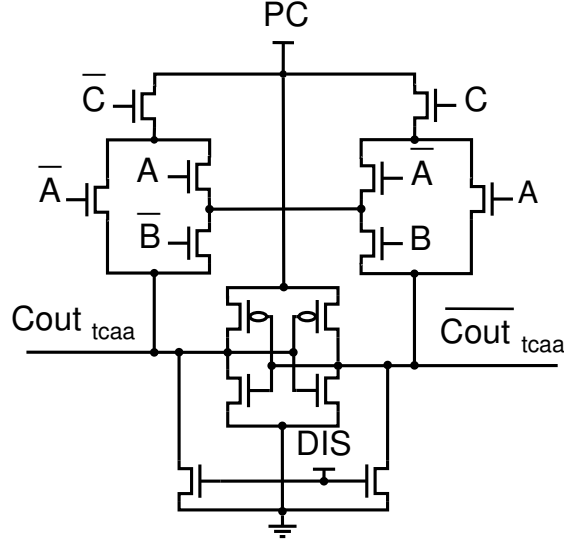
Figure 4.3: EE-SPFAL based True Carryout Approximate Adder(© 2021 IEEE).

4.2 Simulation Results and Discussion

For comparison purposes, this section uses EE-SPFAL-based TSAA and TCAA, CMOS-based Accurate Mirror Adder (AMA) [1] and CMOS-based approximate mirror adders [2]. The proposed designs are evaluated in terms of power, energy, area, and security against Differential Power Analysis (DPA) attacks. The simulations are performed with 45 nm technology. The width of PMOS is used as 240 nm, and the width of NMOS is used as 120 nm for CMOS simulation. The width of PMOS as 360 nm and the width of NMOS as 120 nm are used for EE-SPFAL simulation.

4.2.1 Simulations with Different Frequencies

We use the trapezoid waveform for the all inputs to simulate the circuit. The power consumption and energy consumption per cycle by varying the frequency at 10 fF are shown in Table 4.1 and Table 4.2, respectively. The four CMOS based approximate adders presented in [2] are represented as CMOS $Apx1$, CMOS $Apx2$, CMOS $Apx3$ and CMOS $Apx4$ in Table 4.1 and Table 4.2.

As the results in Table 4.1 and Table 4.2 show that EE-SPFAL based TCAA has the lowest power and energy consumption in comparison with the EE-SPFAL based TSAA, CMOS based AMA [1] and the CMOS based approximate mirror adders [2]. Furthermore, the EE-SPFAL based TCAA is more power and energy-efficient than the EE-SPFAL based TSAA. Compared to the standard CMOS based AMA, the EE-SPFAL based TSAA achieves 95.40% power-saving and 90.80% energy savings at 12.5 MHz. Additionally, compared to the standard CMOS based AMA, the EE-SPFAL based TCAA achieves 95.48% power-saving and 90.96% energy savings. In comparison, EE-SPFAL based TCAA based yields more power and energy savings at a higher frequency than EE-SPFAL based TSAA.

Table 4.1: Power consumption (nW) of EE-SPFAL based proposed designs and CMOS based adders at different frequencies (© 2021 IEEE).

Frequency (MHz)	1	12.5	25	50
CMOS AMA [1]	25.46	273.2	440.5	786.8
CMOS $Apx1$ [2]	17.98	201.0	344.0	559.8
CMOS $Apx2$ [2]	17.16	207.8	415.2	762.1
CMOS $Apx3$ [2]	11.39	138.9	278.3	557.5
CMOS $Apx4$ [2]	15.12	171.2	313.6	591.7
EE-SPAL TSAA	0.539	12.57	33.28	88.97
EE-SPAL TCAA	0.542	12.35	32.54	86.83

Table 4.2: Energy Per Cycle (fJ/Cycle) of EE-SPFAL based proposed designs and CMOS based adders at different frequencies (© 2021 IEEE).

Frequency (MHz)	1	12.5	25	50
CMOS AMA [1]	12.73	10.93	8.810	7.868
CMOS $Apx1$ [2]	8.991	8.043	6.880	5.598
CMOS $Apx2$ [2]	8.581	8.313	8.304	7.621
CMOS $Apx3$ [2]	5.695	5.558	5.566	5.575
CMOS $Apx4$ [2]	7.558	6.846	6.273	5.916
EE-SPFAL TSAA	0.539	1.006	1.331	1.780
EE-SPFAL TCAA	0.541	0.988	1.301	1.736

4.2.2   Simulations with Different Load Capacitance

We conducted further simulations to test the drive strengths of the suggested adiabatic approximate adders by adjusting the load capacitance at 12.5 MHz. Fig.4.4 and Fig.4.5 show that EE-SPFAL based TCAA is more power and energy efficient than EE-SPFAL based TSAA. Table 4.3 and Table 4.4 present the power and energy comparison results of the EE-SPFAL based TSAA and EE-SPFAL based TCAA. The power consumption is 21.1 nW, and 20.62 nW for EE-SPFAL based TSAA and EE-SPFAL based TCAA with a 15 fF load capacitance. Also, EE-SPFAL based TSAA and EE-SPFAL based TCAA with a load capacitance of 15 fF has energy per cycle of 1.689 fJ/cycle and 1.649 fJ/cycle, respectively. The simulation validated that the EE-SPFAL based TCAA is less sensitive to the load capacitance changes compare to EE-SPFAL based TSAA.

Table 4.3: Power consumption (nW) of CMOS AMA, EE-SPFAL based TSAA and EE-SPFAL based TCAA with different load capacitance (© 2021 IEEE).

Load Capacitance (fF)	5	10	15
CMOS AMA [1]	153.8	273.2	362.5
EE-SPFAL TSAA	5.918	12.57	21.10
EE-SPFAL TCAA	5.916	12.35	20.62

Table 4.4: Energy Per Cycle (fJ/Cycle) of CMOS AMA, EE-SPFAL based TSAA and EE-SPFAL based TCAA with different capacitance loads (© 2021 IEEE).

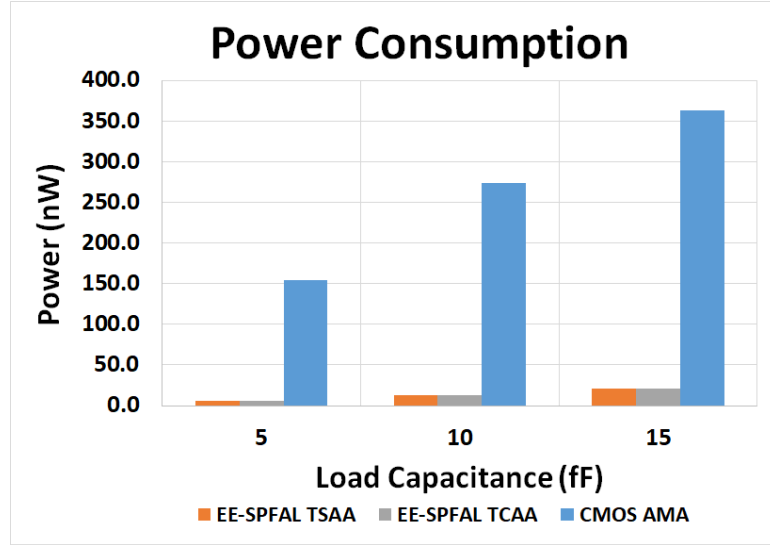| Load Capacitance (fF)	5	10	15
CMOS AMA [1]	6.15	10.93	14.50
EE-SPFAL TSAA	0.473	1.006	1.689
EE-SPFAL TCAA	0.473	0.988	1.649

Figure 4.4: Power Consumption (nW) of EE-SPFAL based TSAA, EE-SPFAL based TCAA and CMOS AMA (© 2021 IEEE)
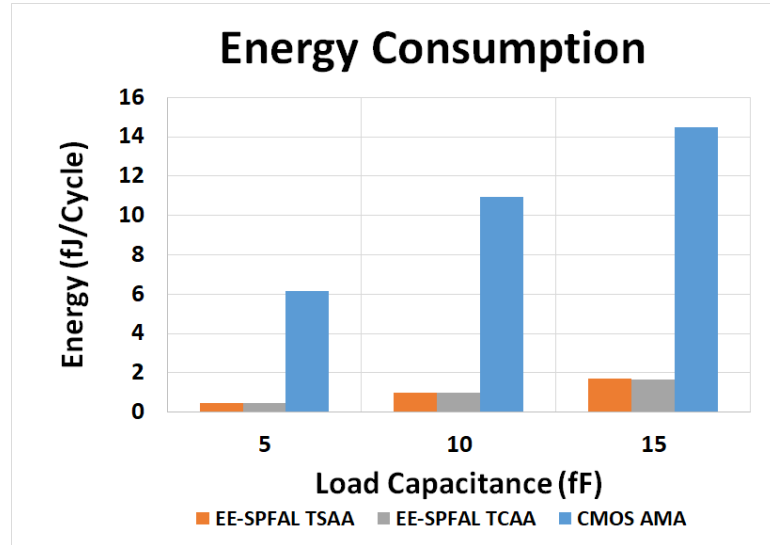

Figure 4.5: Energy Consumption (fJ/Cycle) of EE-SPFAL based TSAA, EE-SPFAL based TCAA and CMOS AMA (© 2021 IEEE).

4.2.3 Evaluation in Number of Transistors

The transistor count of the traditional CMOS-based accurate mirror adder (AMA) [1], CMOS-based approximate mirror adders [2], EE-SPFAL-based TSAA, and EE-SPFAL-based TCAA is shown in the Table 4.5. From Table 4.5, both proposed designs have less transistor than CMOS based AMA. EE-SPFAL based TSAA has 33% fewer transistors, and EE-SPFAL based TCAA has 41.7% fewer transistors compared to CMOS AMA.

Table 4.5: Transistors count in EE-SPFAL based TSAA, TCAA and CMOS based adders (© 2021 IEEE).

	PMOS	NMOS	Total
CMOS AMA [1]	12	12	24
CMOSapx1 [2]	8	8	16
CMOSapx2 [2]	7	7	14
CMOSapx3 [2]	6	5	11
CMOSapx4 [2]	5	6	11
EE-SPFAL TSAA	2	14	16
EE-SPFAL TCAA	2	12	14

4.2.4 Mean Error Distance

In this section, we are presenting the accuracy of both proposed adders. The Mean Error Distance (MED) is the metric to determine the accuracy of the approximate circuits. The accuracy is inversely proportional to the MED value. The smaller the MED value, the better is the accuracy of the approximate circuit. The MED values are computed with equation 4.3; where Error Distance (ED) is the difference between the exact output and the approximate output for a given input, P is the probability of the ED, n is the number of bit of the adder.

$$ED = |Out_{acu} - Out_{apx}|$$

$$MED = \sum_n EDs_n * P(EDs_n) \tag{4.3}$$

Table 4.6 presents the MED value of approximate adders. The MED value of EE-SPFAL based 4-bit TCAA is 3.617, which is the 2nd lowest value. However, the MED value of EE-SPFAL based 4 bits TSAA is 5.515, which is the highest value among all approximate adders. We can conclude that the EE-SPFAL based TCAA has better accuracy than EE-SPFAL based TSAA.

Table 4.6: MED value of EE-SPFAL based TSAA, TCAA and CMOS based approximate adders (© 2021 IEEE).

	1 bit adder	4 bit adder
CMOS$apx1$ [2]	0.250	2.719
CMOS$apx2$ [2]	0.250	3.617
CMOS$apx3$ [2]	0.500	4.426
CMOS$apx4$ [2]	0.375	5.000
EE-SPFAL TSAA	0.500	5.515
EE-SPFAL TCAA	0.250	3.617

4.2.5 Resistance Against Differential Power Analysis Attack

We present the simulation results of the EE-SPFAL based TCAA and TSAA to evaluate their resistance against DPA attack. Simulations were performed at 45 nm technology node with the load capacitance of 10 fF. Figure 4.6 shows the uniform current profile of the EE-SPFAL based TCAA and TSAA adders.

For determining the ability of the TCAA and TSAA to resist the DPA attack, two parameters are calculated for all possible input combinations. The first parameter is the Normalized Energy Deviation (NED), which is the percentage difference between the minimum and maximum energy consumption. The second parameter is
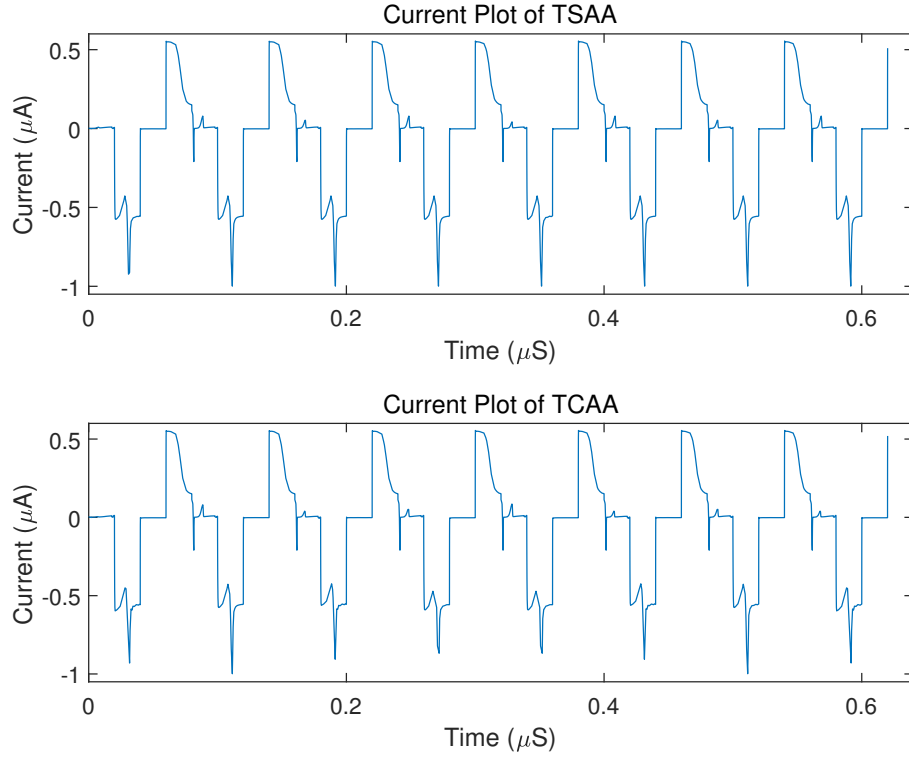
Figure 4.6: Current waveform of TSAA and TCAA (© 2021 IEEE).

Normalized Standard Deviation (NSD) which is the energy consumption variation. The formulas to calculate NED and NSD are listed in equation 4.4; σ_E is the standard deviation of energy consumption and E_{avg} is the average energy consumption.

$$NED = \frac{(E_{max} - E_{min})}{E_{max}}$$
$$NSD = \frac{\sigma_E}{E_{avg}} \tag{4.4}$$

Table 4.7 presents the NED and NSD values of the TCAA and TSAA. The EE-SPFAL based TSAA has a lower NED and NSD value which indicates EE-SPFAL based TSAA has more balanced energy consumption and is more secure than EE-SPFAL based TCAA. The larger NED and NSD value of EE-SPFAL based TCAA is due to the variation of intrinsic capacitance when different inputs are given. We

found out that increasing the load capacitance of EE-SPFAL based TCAA improves the NED and NSD value. However, the NED and NSD value of EE-SPFAL based TCAA is more than 30 times higher than EE-SPFAL based TSAA.

Table 4.7: Normalized energy deviation and normalized standard deviation of TSAA and TCAA (© 2021 IEEE).

	TCAA	TSAA
$E_{max}(J)$	1.41E-15	1.53E-15
$E_{min}(J)$	1.60E-15	1.54E-15
NED (%)	11.83	0.275
NSD (%)	3.660	0.102

4.3   Summary

In this chapter, we illustrated that low-power and secure solutions for edge computing could be developed by the hybridization of approximate computing and adiabatic logic. Based on dual-rail adiabatic logic, two novel adiabatic approximate adders are proposed. The findings show a substantial decrease in power and energy consumption in the approximate adders based on adiabatic logic compared to the traditional CMOS design. Furthermore, proposed adders have uniform power consumption, which increases the resistance against the DPA attack. Therefore, it is concluded that the proposed adiabatic True Carry-out Approximate Adder (TCAA) offers more energy and power savings, has fewer transistors and has better accuracy. However, the adiabatic True Sum Approximate Adder (TSAA) offers a more uniform waveform that increases the resistance to DPA attacks.

Chapter 5

Conclusion and Future Work

In this thesis, significant contributions are made towards approximation computing in adiabatic logic to offers low-power and energy-efficient solutions with enhanced security.

The first contribution is the proposal of two novel approximated adiabatic adders. The Positive Feedback Adiabatic Logic (PFAL) based approximate adder has a significant decrease in power and energy consumption compared to the traditional CMOS design. Further, PFAL based approximate adders have less transistor when compare to CMOS AMA and reduce the drawback of doubling the number of transistors when applying adiabatic logic. The second contribution is the proposal of approximate adiabatic logic with enhanced security. The Energy-Efficient Secure Positive Feedback Adiabatic Logic (EE-SPFAL) based approximate adders have uniform power consumption, which increases the resistance against the DPA attack.

Furthermore, EE-SPFAL adders have a substantial decrease in power and energy consumption compared to conventional CMOS design. Therefore, it is concluded the adiabatic True Carry-out Approximate Adder (TCAA) offers more saving in power and energy. In contrast, the EE-SPFAL based True Sum Approximate Adder (TSAA) shows a more uniform waveform.

The designs proposed in this thesis provide a possible path for future work. One such direction would be designing adiabatic logic-based approximate compressors and multipliers. Another possible future work could be applying adiabatic-based approximations on emerging nanotechnology devices, like FinFET, for further saving. Additionally, the adiabatic logic-based approximations can be implemented on a spintronic device, such as Magnetic Tunnel Junction (MTJ), for reduced leakage loss.

Bibliography

[1] Neil Weste and David Harris. *CMOS VLSI Design: A Circuits and Systems Perspective*. Addison-Wesley Publishing Company, USA, 4th edition, 2010.

[2] Vaibhav Gupta, Debabrata Mohapatra, Anand Raghunathan, and Kaushik Roy. Low-power digital signal processing using approximate adders. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 32(1):124–137, 2012.

[3] S Dinesh Kumar, Himanshu Thapliyal, and Azhar Mohammad. Ee-spfal: A novel energy-efficient secure positive feedback adiabatic logic for dpa resistant rfid and smart card. *IEEE Transactions on Emerging Topics in Computing*, 7(2):281–293, 2016.

[4] Felipe Caro and Ramin Sadr. The internet of things (iot) in retail: Bridging supply and demand. *Business Horizons*, 62(1):47–54, 2019.

[5] Jiasi Chen and Xukan Ran. Deep learning with edge computing: A review. *Proceedings of the IEEE*, 107(8):1655–1674, 2019.

[6] AA Raneesha Madushanki, Malka N Halgamuge, WAH Surangi Wirasagoda, and Ali Syed. Adoption of the internet of things (iot) in agriculture and smart farming towards urban greening: A review. 2019.

[7] Cisco Visual Networking. Cisco global cloud index: Forecast and methodology, 2015-2020. white paper. *Cisco Public, San Jose*, 2016.

[8] Sam Lucero et al. Iot platforms: enabling the internet of things. *White paper*, 2016.

[9] Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, and Xinyu Yang. A survey on the edge computing for the internet of things. *IEEE access*, 6:6900–6919, 2017.

[10] Joseph Azar, Abdallah Makhoul, Mahmoud Barhamgi, and Raphaël Couturier. An energy efficient iot data compression approach for edge machine learning. *Future Generation Computer Systems*, 96:168–175, 2019.

[11] Wu Yang and Himanshu Thapliyal. Low-power and energy-efficient full adders with approximate adiabatic logic for edge computing. In *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 312–315, 2020.

[12] Wu Yang and Himanshu Thapliyal. Approximate adiabatic logic for low-power and secure edge computing. *IEEE Consumer Electronics Magazine*, pages 1–1, 2021.

[13] Cole Terrell and Himanshu Thapliyal. Approximate adder circuits using clocked cmos adiabatic logic (ccal) for iot applications. In *2020 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–4. IEEE, 2020.

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

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

[16] J Fischer, E Amirante, A Bargagli-Stoffi, and D Schmitt-Landsiedel. Improving the positive feedback adiabatic logic familiy. *Advances in radio Science*, 2(D. 1):221–225, 2005.

[17] Joonho Lim, Kipaek Kwon, and Soo-Ik Chae. Reversible energy recovery logic circuit without non-adiabatic energy loss. *Electronics Letters*, 34(4):344–345, 1998.

[18] G Joy Persial, M Prabhu, and R Shanmugalakshmi. Side channel attack-survey. *Int J Adva Sci Res Rev*, 1(4):54–57, 2011.

[19] S Dinesh Kumar, Himanshu Thapliyal, Azhar Mohammad, and Kalyan S Perumalla. Design exploration of a symmetric pass gate adiabatic logic for energy-efficient and secure hardware. *Integration*, 58:369–377, 2017.

[20] Zachary Kahleifeh and Himanshu Thapliyal. Adiabatic logic based energy-efficient security for smart consumer electronics. *IEEE Consumer Electronics Magazine*, 2020.

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

[22] Pruthvy Yellu, Novak Boskov, Michel A Kinsy, and Qiaoyan Yu. Security threats in approximate computing systems. In *Proceedings of the 2019 on Great Lakes Symposium on VLSI*, pages 387–392, 2019.

[23] Francesco Regazzoni, Cesare Alippi, and Ilia Polian. Security: the dark side of approximate computing? In *2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 1–6. IEEE, 2018.

[24] Mingze Gao, Qian Wang, Md Tanvir Arafin, Yongqiang Lyu, and Gang Qu. Approximate computing for low power and security in the internet of things. *Computer*, 50(6):27–34, 2017.

Vita

Wu Yang

Education

University of Kentucky

Bachelor of Science in Electrical Engineering, May 2019

Experience

Graduate Teaching Assistant

August 2019 - May 2021

University of Kentucky

Lexington, KY

Publications

Yang, Wu, and Himanshu Thapliyal. "Approximate Adiabatic Logic for Low-Power and Secure Edge Computing." IEEE Consumer Electronics Magazine (2021).

Yang, Wu, and Himanshu Thapliyal. "Low-Power and Energy-Efficient Full Adders With Approximate Adiabatic Logic for Edge Computing." In 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 312-315. IEEE, 2020.