2018

EMERGING COMPUTING BASED NOVEL SOLUTIONS FOR DESIGN OF LOW POWER CIRCUITS

Azhar Mohammad
University of Kentucky, azhar.mohammad@uky.edu
Digital Object Identifier: https://doi.org/10.13023/etd.2018.456

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.

Azhar Mohammad, Student

Dr. Himanshu Thapliyal, Major Professor

Dr. Aaron Cramer, Director of Graduate Studies

EMERGING COMPUTING BASED NOVEL SOLUTIONS FOR DESIGN OF LOW POWER CIRCUITS

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
Azhar Mohammad
Lexington, Kentucky
Director: Dr. Himanshu Thapliyal
Lexington, Kentucky
2018

ABSTRACT OF THESIS

EMERGING COMPUTING BASED NOVEL SOLUTIONS
FOR DESIGN OF LOW POWER CIRCUITS

The growing applications for IoT devices have caused an increase in the study of low power consuming circuit design to meet the requirement of devices to operate for various months without external power supply. Scaling down the conventional CMOS causes various complications to design due to CMOS properties, therefore various non-conventional CMOS design techniques are being proposed that overcome the limitations. This thesis focuses on three of those emerging and novel low power design techniques namely Adiabatic logic and Magnetic Tunnel Junction (MTJ) logic and Carbon Nanotube Field Effect transistor (CNFET) logic. Circuits that are used for large computations (multipliers, encryption engines) that amount to maximum part of power consumption in a whole chip are designed using these novel low power techniques.

KEYWORDS: Adiabatic logic, Differential Power Analysis, Magnetic Tunnel Junction, Carbon Nanotube Field effect Transistor.

Azhar Mohammad

December 5, 2018

EMERGING COMPUTING BASED NOVEL SOLUTIONS
FOR DESIGN OF LOW POWER CIRCUITS

By

Azhar Mohammad

Dr. Himanshu Thapliyal

(Director of Thesis)

Dr. Aaron Cramer

(Director of Graduate Studies)

December 5, 2018

(Date)

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

The "Internet of things" (IoT) is a concept that was developed in early 2000's according to which any device with a wireless connection can be connected to the Internet (and/or to each other) [3]. This includes cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and many more. This was a challenge back then due to limitations in the technology. But now, with all the advancements, the IoT has gained a lot of attention as it proved to change the human lives for better by creating the pathway for smart homes, cities etc. As of now 23.14 billion devices are connected and there is an estimation that by 2025 the connected devices will be over 75 billion [4]. The IoT application space is characterized by two overarching design concerns [5]. One, the IoT devices are frequently in locations without easy access to power, therefore most of the devices are battery powered that constraints the life time of the device [6]. So, low power consumption is the most universal constraint across the IoT space. The scaling of CMOS technology lowered the power consumption significantly, which makes the recent efforts in IoT applications feasible with a decent battery capacity. However further power reduction becomes more and more challenging because further voltage scaling in CMOS to reduce the dynamic computation power while providing sufficient speed conflicts with the exponentially

increasing leakage power. This fundamentally limits the growth of functionality and scenarios where IoT devices are powered by batteries or harvested energy.

Security is another concern in IoT sphere. Often times there are scenarios where all objects (including sensors, wearable devices, appliances) send data to hosts via an insecure wireless network. In order to provide secure communications crypto algorithms are widely adopted in WSNs (Wireless Sensor Networks) [7]. Side-channel attacks, Differential Power Analysis in particular directly relates circuit architectures and data-dependent power consumption profile. Such attacks when performed on RFID chips in credit cards, reveal the encryption key thus enabling the attacker to steal the victim's sensitive financial information. Therefore the IoT devices must be resistant to such attacks.

The focus of this thesis is to explore various emerging novel solutions which can be used in low power computing. This thesis talks about adiabatic logic which is perfect to design circuits for IoT applications since power clocks are used to efficiently recover the charge stored in the load capacitors thus allowing to create ultra low power circuits. Also the adiabatic logic helps to eliminate the data power dependency thus making it secure to DPA attacks. Spin based devices are emerging devices well suited to design low power circuits because of their promising characteristics such as near-zero standby power, non-volatility, high integration density, etc. Among Spin based devices Magnetic Tunnel junction (MTJ) is quite extensively used because of their superior properties such as high sensitivity, low-cost, low-power, compatibility with complementary metaloxide semiconductor (CMOS) technology, and room-temperature operation [8]. An upcoming novel device is Carbon Nanotube Field Effect Transistor (CNFET) which is essentially a brilliant alternative to CMOS in designing low power circuits. CNFETs are formed in cylindrical shape with sheets of graphite tubes. Some of the advantages of CNFETs are such as they have higher ON current compared to MOSFET transistors. Also, ballistic conduction of CNFETs

reduces the power dissipation in the transistor body.

1.1 Contribution of Thesis

The major contributions of this thesis is design of low power computing and cryptographic circuits using novel computing paradigms of Adiabaltic Logic, MTJ/CMOS and MTJ/CNFET. Below is a brief summary of the contributions of this thesis. It also presents both CMOS/MTJ and CNFET/MTJ based hybrid compressor circuits. Compressors are used to reduce the accumulation of partial products in a multiplier which accounts for major share of power consumption.

1. Proposal of a novel family of Adiabatic logic called Symmetric Pass Gate Adiabatic Logic (SPGAL). This proposed logic was used to design Buffer, AND/NAND, XOR/XNOR gates. These logic gates reduce the power consumption by 80% when compared to adiabatic families in current literature which suffer from non-adiabatic losses.

2. Implementation of Bit-Parallel Cellular Multiplier over $GF(2^4)$ using SPGAL gates. Galois multipliers play a major role in the engineering applications such as cryptography and error correcting codes. The simulation results show that multiplier design using SPGAL gates saves upto 81% energy.

3. Implementation of AES S-Box circuit using SPGAL gates. S-Box is an integral part of encryption engines that converts plain inputs to encrypted outputs. The SPGAL S-Box saves upto 91% energy when compared to CMOS logic.

4. Proposal of a 4-2 compressor circuit in hybrid CMOS/MTJ and cascaded 4-2 compressor circuit in hybrid CNFET/MTJ. These designs show a significant energy reduction of 50% and 80% respectively compared to compressors designed using CMOS logic.

1.2 Outline of Thesis

Chapter 2 provides an overview of Adiabatic Logic, Differential Power Analysis Attack, MTJ and CNFET. Chapter 3 presents designs of a Symmetric Pass Gate Adiabatic gates, implementation of GF multiplier, implementation and DPA attack on a AES S-box using the proposed SPGAL gates . Chapter 4 presents design of proposed 4-2 compressor in hybrid CMOS/MTJ and CNFET/MTJ. Chapter 5 concludes the thesis. Designs from chapter 3 were previously published in [9] (© [2018] Elsevier) and [10] (© [2018] IEEE) . Designs from chapter 4 were previously published in [11] (© [2018] Elsevier).

Chapter 2

Background

This chapter will cover any background information needed to understand the successive chapters. The main focus will be on adiabatic logic, spintronic devices (MTJ), Carbon Nanotube Field Effect Transistor (CNFET) and Differential Power Analysis attack.

2.1 Adiabatic Logic

Adiabatic logic recycles the charge stored in the load capacitor back to the power clock which reduces the overall energy consumed by the circuit. Fig. 2.1 shows the adiabatic charging of the load capacitor and its recovery path. The energy dissipated in an adiabatic circuit when considering the charge is supplied through a constant current source is shown by,

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

Where T is the charging/discharging time of the capacitor, C is the load capacitor, R is the parasitic resistance of the transistors, V_{dd} is the full swing of the power clock. If the T $\gg$ 2RC (time constant), the energy dissipated by the adiabatic circuit is less than the conventional CMOS circuit. However there are certain challenges to design

using Adiabatic logic and they are to recognize different types of losses in adiabatic circuits. They are adiabatic loss, non-adiabatic loss and leakage loss.

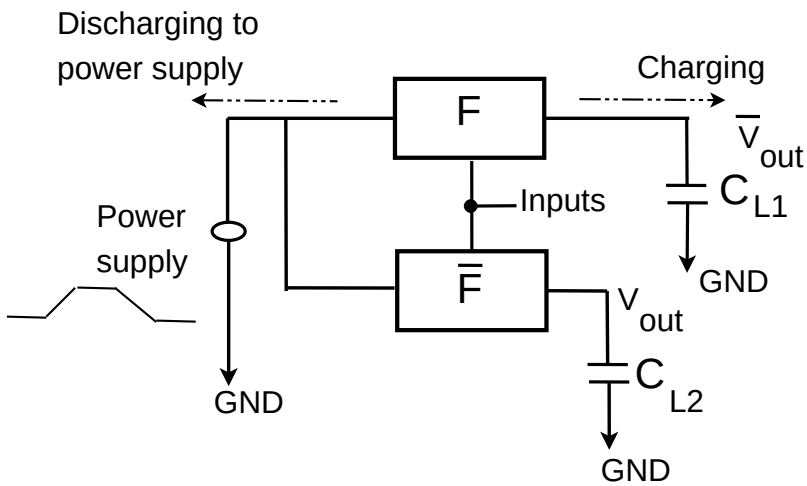


Figure 2.1: Adiabatic charging/discharging[1]

Adiabatic loss

Fig. 2.2(a) illustrates the switch model for the adiabatic loss. When the switch (SW) is turned on, the adiabatic loss is shown by,

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

where R_{on} is the on-resistance of the switch, T is the transition period and C_L is the load capacitance. From equation 2.1, it can be seen that the adiabatic loss can be

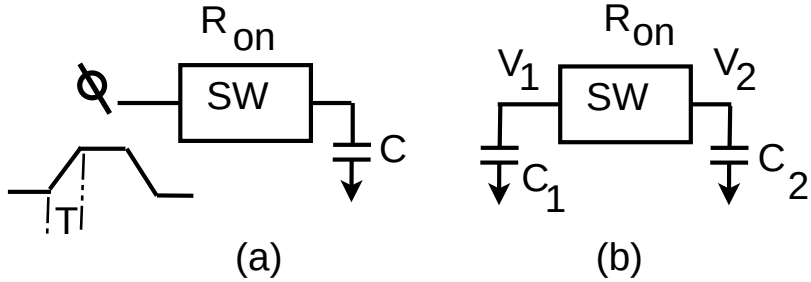


Figure 2.2: illustrates the switch model for a) adiabatic loss b) non-adiabatic loss

eliminated, if the transition period (T) reaches infinity. In practice, it is impossible to make the transition period (T) to infinity. It is concluded that adiabatic loss is unavoidable and can be reduced with the low frequency operated circuits [1]. In this work, we are targeting the application of IoT devices which will operate at low frequencies. Hence, these designs will have low adiabatic loss.

Non-adiabatic loss

Fig. 2.2(b) shows the switch model to depict the non-adiabatic loss. If any voltage difference between two terminals of a switch exists when it is turned on, non-adiabatic loss occurs. Non-adiabatic loss is shown by,

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

Where C_1 and C_2 are the capacitances of the two nodes connected to the switch and V_1 and V_2 are the voltages at the two nodes just before the switch is turned on. For the low speed operation circuits, non-adiabatic loss is much higher than the adiabatic loss [12]. In order to avoid non-adiabatic loss, transistor should not turn ON if there is any potential difference between the drain and source (two nodes) of the transistor.

2.2 Differential Power Analysis Attack

Differential Power Analysis attack exploits the data leakage from the devices. No matter how secure a cryptographic algorithm might be, its implementation on a chip may be insecure because of unpredictable data leakage. Any change of state of a CMOS gate can be measured on the VDD or VSS pins that reveal an intermediate data being processed by the cryptographic device. For a successful Differential Power Analysis attack one needs [13]:

- the measurements of the power consumption;

- the encryption algorithm used;

- a set of plaintexts or cipher texts.

The mathematical model of the power consumption at time t is equal to the sum of the power dissipated of all gates at same time [14]. In Equation 2.4 is represented a simplified mathematical model of power consumption:

$$P(t) = \Sigma_g f(g,t) + N(t) \tag{2.4}$$

The function $f(g,t)$ represents the power consumption of the gate g at the time t and the function $N(t)$ represents the noise components.

2.2.1 Differential Power Analysis Attack Process

The DPA attack is done by measuring the power consumption while 'd' different plain texts are encrypted. The known current trace values are written as a vector $i = (i_1, i_2, ..., i_d)$, where i_n denotes the current trace value of the nth input plain text. During each run of the input plain text encryption, current traces are collected and sampled. The sampled current trace values that corresponds to a particular input plain text is given as $t_i = (t_{i,1}, t_{i,2}, ..., t_{i,T})$ where T denotes the length of the trace. A dXT matrix is created that stores this current samples. Next a hypothetical power consumption matrix using Hamming distance/Hamming weight of the cipher text is created where $H(i,k) = \Sigma_{j=0}^{m-1} HD(O_{i,k}, O_{i-1,k})$.

$HD(O_{i,k}, O_{i-1,k})$ represents the hamming distance between i^{th} and i-1th cipher text.

$$H_{(i,k)} = \begin{bmatrix} H_{0,0} & H_{0,1} & H_{0,2} & \dots & H_{0,k-1} \\ H_{1,0} & H_{1,1} & H_{1,2} & \dots & H_{1,k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ H_{d-1,0} & H_{d-1,1} & H_{d-1,2} & \dots & H_{d-1,k-1} \end{bmatrix}$$

In the matrix $H(i, K)$, HD values are the number of bits that differ between two consecutive outputs. Finally each column of the H matrix is compared with the each column of the M matrix i.e the hypothetical power consumption values for all the keys are compared with recorded traces at different instances of time. This will result in an another matrix R which is of size KXT. Each element of R matrix ($r_{i,j}$) contains the comparison result between the columns of h_i and m_j.

$$r_{i,j} = \frac{\Sigma_{d=1}^{D}(h_{d,i} - \overline{h_i}).(m_{d,j} - \overline{m_j})}{\sqrt{\Sigma_{d=1}^{D}(h_{d,i} - \overline{h_i})^2.(m_{d,j} - \overline{m_j})^2}} \tag{2.5}$$

$$R = \begin{bmatrix} r_{0,0} & r_{0,1} & r_{0,2} & \cdots & r_{0,t} \\ r_{1,0} & r_{1,1} & r_{1,2} & \cdots & r_{1,t} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{k-1,0} & r_{k-1,1} & r_{k-1,2} & \cdots & r_{k-1,t} \end{bmatrix}$$

2.3 Magnetic Tunnel Junction

Magnetic Tunnel Junction (MTJ) is a spin based device which is most suited to use in Logic In Memory architectures because of its short access time, small dimensions and compatibility with CMOS technology. The structure of MTJ is a vertical nanopillar that consists of two ferromagnetic (FM) layers and an oxide barrier [15]. In the standard application of MTJ devices, the magnetization of one of the FM layers is fixed, while the other FM layer is free to take one of the two orientations (parallel and antiparallel) as shown in Fig. 2.3 [16].

Depending on the orientation of the FM layers, parallel (P) or antiparallel (AP), MTJ device shows either a low resistance (RP) or high resistance (RAP) characteristic. The resistance difference between the two configurations of MTJ device is given by the tunnel magnetoresistance ratio $TMR = (R_{AP} - R_P)/R_P$.

Spin transfer torque (STT) is one of the promising methods to switch MTJs [17].

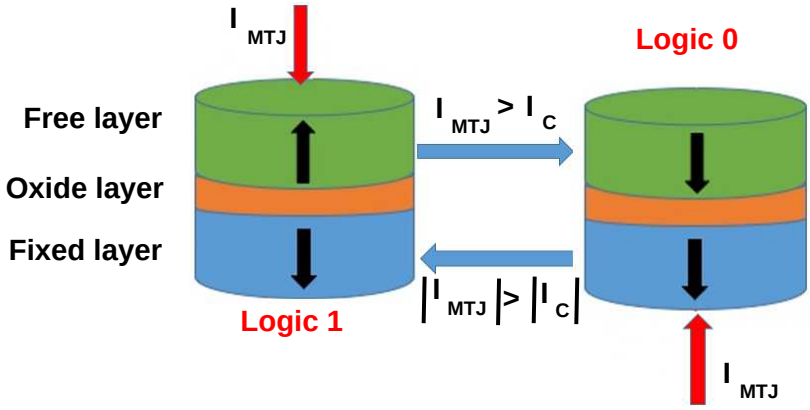


Figure 2.3: Vertical Magnetic Tunnel Junction (MTJ) nanopillar structure. MTJ states change from P to AP and vice versa by applying proper current.

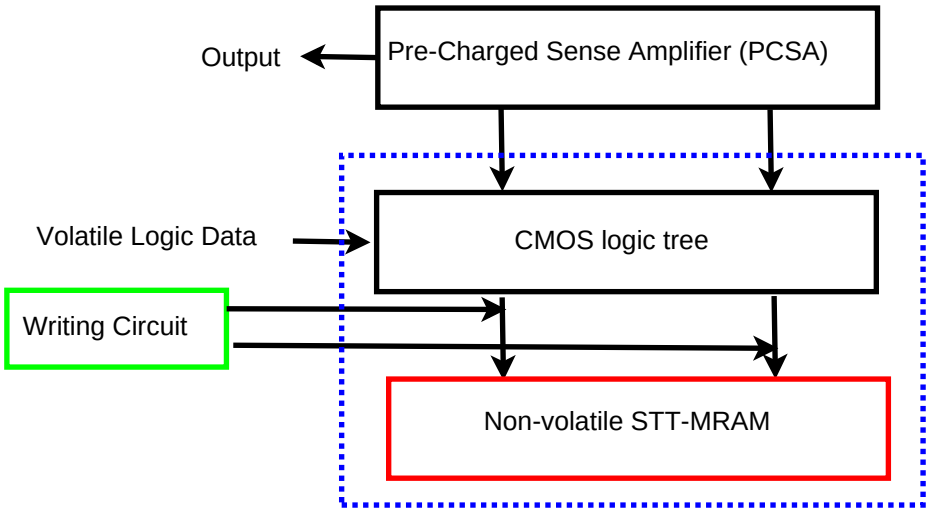


Figure 2.4: Structure of a MTJ based circuit

Further, STT switching mechanism requires only a bidirectional current to switch the orientations in MTJs. The states of the MTJ are switched when the current of the MTJ (I_{MTJ}) becomes higher than a critical current (I_C) (Fig. 2.3) [18].

The first part is the writing circuit, which is used for programing memory elements. The second part consists of STT-MRAM cells and a CMOS logic tree. STT-MRAM cells are used to store data and the CMOS logic tree is used as a logic control block. Finally, the last part is a sense amplifier (SA) that evaluates the output logic results. The pre-charged sense amplifier (PCSA) is a clock based circuit and is utilized in the MTJ based circuits because of its low power consumption and high reliability.

2.4 Carbon Nanotube Field Effect Transistor

CNFETs are formed in the shape of a sheet of graphite tubes. Some of the advantages of CNFETs are such as they have higher ON current compared to MOSFET transistors. Also, ballistic conduction of CNFETs reduces the power dissipation in the transistor body. One dimension structure of CNTs reduces the resistivity and consequently the energy and the power dissipation. CNTs are grouped into Single-Walled Carbon Nano Tube (SWCNT) and Multi-Walled Carbon Nano Tube (MWCNT). SWCNTS are made of one cylinder and MWCNTs are made of more than one cylinder that are nested inside each other [19].

Several SWCNTs can be placed next to each other under the transistor gate and its width. The width of CNFET transistor depends on the number of tubes which are placed under the transistor gate. The width of the CNFET transistor also depends on the distance between two adjacent tubes which is called a pitch. The width of the CNFET transistor is given by the following equation [20]:

$$W_{gate} \cong Min(W_{min}, N \times pitch) \tag{2.6}$$

Where, N is the number of nanotubes that are placed under the transistor gate and W_{min} is the minimum width of the gate.

Threshold voltage of the CNFET transistors is determined by the following equations [20]:

$$V_{th} \cong \frac{E_g}{2e} = \frac{\sqrt{3}}{3}\frac{aV_\pi}{eD_{CNT}} \cong \frac{0.43}{D_{CNT}(nm)} \tag{2.7}$$

In the above equation, a is the carbon to carbon atom distance, V_π is the carbon $\pi - \pi$ band energy in the tight bonding model, e is the unit electron charge and D_{CNT} is the diameter of the CNFETs.

Chapter 3

Design of Symmetric Pass gate Adiabatic Logic Circuits

Khatir et. al proposed Secure Adiabatic Logic (SAL) [21] which is not only energy efficient in nature but also resistance against side-channel attacks. This adiabatic logic uses pass transistors to discharge the internal parasitic capacitances to balance the peak current traces. But extensive analysis made in [22] reports that SAL logic exhibit supply current dependences. Choi et. al proposed Symmetric Adiabatic Logic[23] (SyAL) which has been modified from Efficient Charge Recovery Logic (ECRL)[24]. This logic uses symmetric discharge paths and charge sharing feature to equalize the voltage between the output nodes and the internal nodes. This feature balances the supply current waveforms of this logic. Monterio et. al proposed Charge Sharing Symmetric Adiabatic Logic (CSSAL)[22]. This logic is implemented with charge sharing symmetric input logic structure in SyAL. But CSSAL uses twelve trapezoidal clock sources making their structure more complicated[25]. Recently, Secured Quasi Adiabatic Logic was proposed in [25] which has been modified from ECRL-based[24] adiabatic logic. This design has compact area and low energy consumption as compared to all other DPA resistant adiabatic families. But still this family suffers from

non-adiabatic loss during the evaluation of the outputs.

3.1 Design of Proposed SPGAL logic gates

Any circuit, simple or complex is build using basic logic gates like AND, OR, XOR etc., The following sections will cover the design and working of basic logic gates that are design using adiabatic logic.

3.1.1 SPGAL Buffer

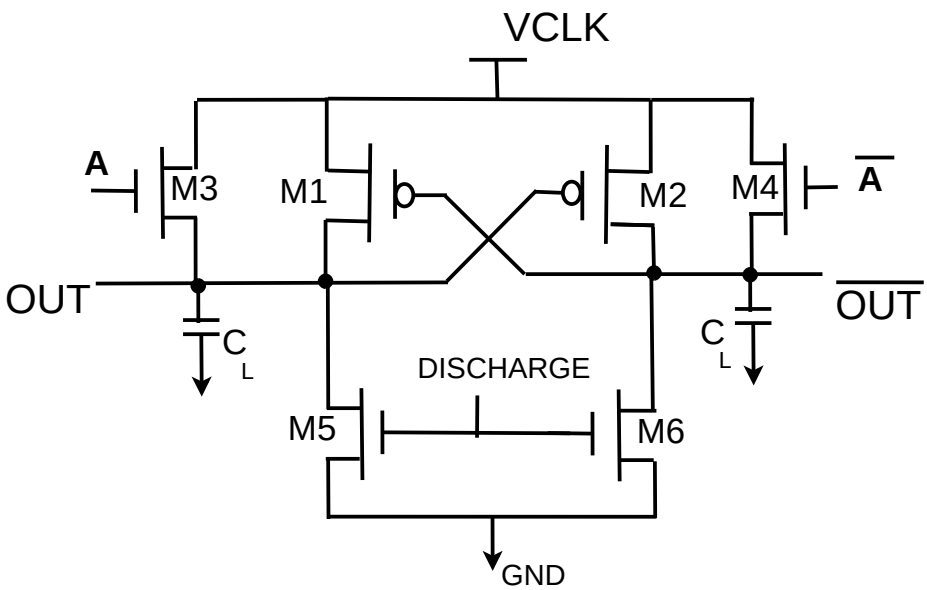


Figure 3.1: SPGAL buffer

Fig. 3.1 shows the buffer design using the proposed Symmetric Pass Gate Adiabatic Logic with the load capacitor of 10fF. The timing diagram for the buffer using SPGAL is shown in Fig. 3.2. The proposed logic family uses a 4-phase trapezoidal clock to efficiently recover the charge stored in the output capacitor. The main intention in designing SPGAL is to eliminate the non-adiabatic loss during the evaluate phase of the outputs. In this family, the load capacitors are charged through the evaluation transistors before the evaluate phase of the next cycle begins. The func-

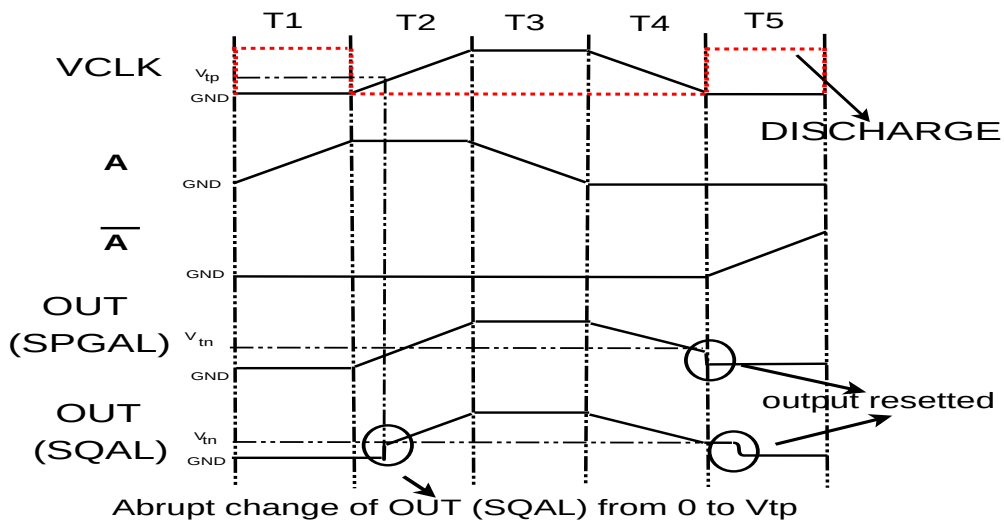


Figure 3.2: Timing diagram for SQAL buffer and SPGAL buffer. DISCHARGE represents the discharge signal. OUT represents the output of the buffer.

tionality of the proposed adiabatic logic family is illustrated by using the design of a buffer. Let us assume that all the nodes are at GND initially.

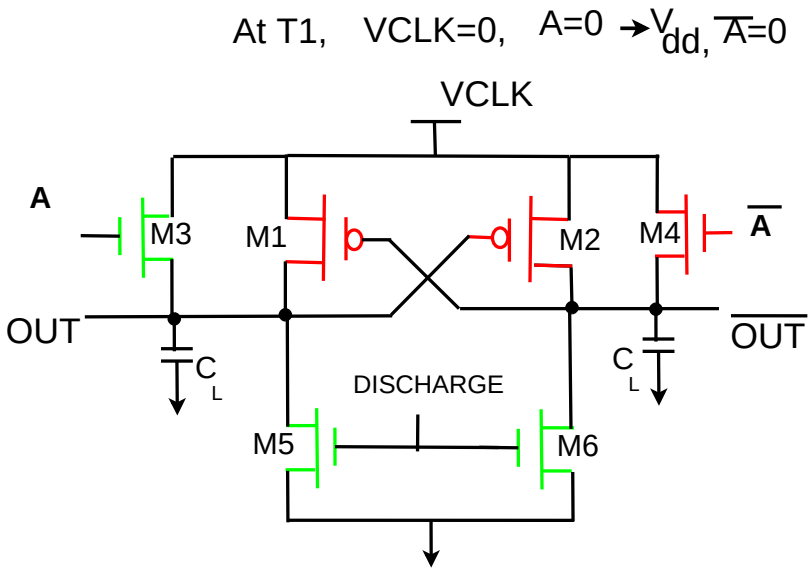


Figure 3.3: Switching operation of transistors in T1 phase of SPGAL buffer for A=1, Ā=0

T1 (Wait phase): At T1, VCLK is at GND. Input A is slowly increasing from 0 to V_{dd}. In general, for NMOS to be turned on, V_{gs} must be greater than V_{tn}, where V_{gs} is the voltage across the gate and the source of the NMOS and V_{tn} is the threshold

voltage of the NMOS. When the input A is greater than V_{tn}, the transistor M3 is turned on. Since the source and drain of M3 is at GND, there will not be any current flow through the transistor. In this phase, discharge signal makes the transistors M5 and M6 to be turned on there by discharging the charges stored (due to previous cycle) in the load capacitor to ground. All other transistors are OFF in this phase. Switching operation of the transistors T1 phase of SPGAL buffer is shown in Fig. 3.3.

T2 (Evaluate Phase): At T2, input A is at V_{dd}. The discharge signal and $\bar{A}$ is at GND. VCLK slowly increases from 0 to V_{dd} which makes the output load capacitor to slowly get charged. At any instant of time, the potential of the clock VCLK will be greater than potential of the output node in this phase. So, the voltage at the output node will always follow the clock VCLK in this phase which makes the OUT node to act as the source and clock to act as the drain of the M3 transistor. For M1, the clock VCLK acts as the source and the OUT node acts as the drain of the transistor. PMOS will be turned on if V_{sg_p} is greater than V_{tp}. For M1 to be turned on, $V_{sg_p} > V_{tp}$.

$$V_{\phi} - V_{\overline{out}} > V_{tp} \tag{3.1}$$

$$V_{\overline{out}} = 0$$

$$V_{\phi} > V_{t_p}$$

So, M1 will be turned on when the clock VCLK reaches V_{tp}. M3 will be tuned off if $V_{GS} < V_{tn}$.

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

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

When OUT reaches $V_{dd} - V_{tn}$, M3 will be turned off and the current will flow through M1 to charge the load capacitor. Fig. 3.4 shows the switching operation of the transistors in T2 phase.

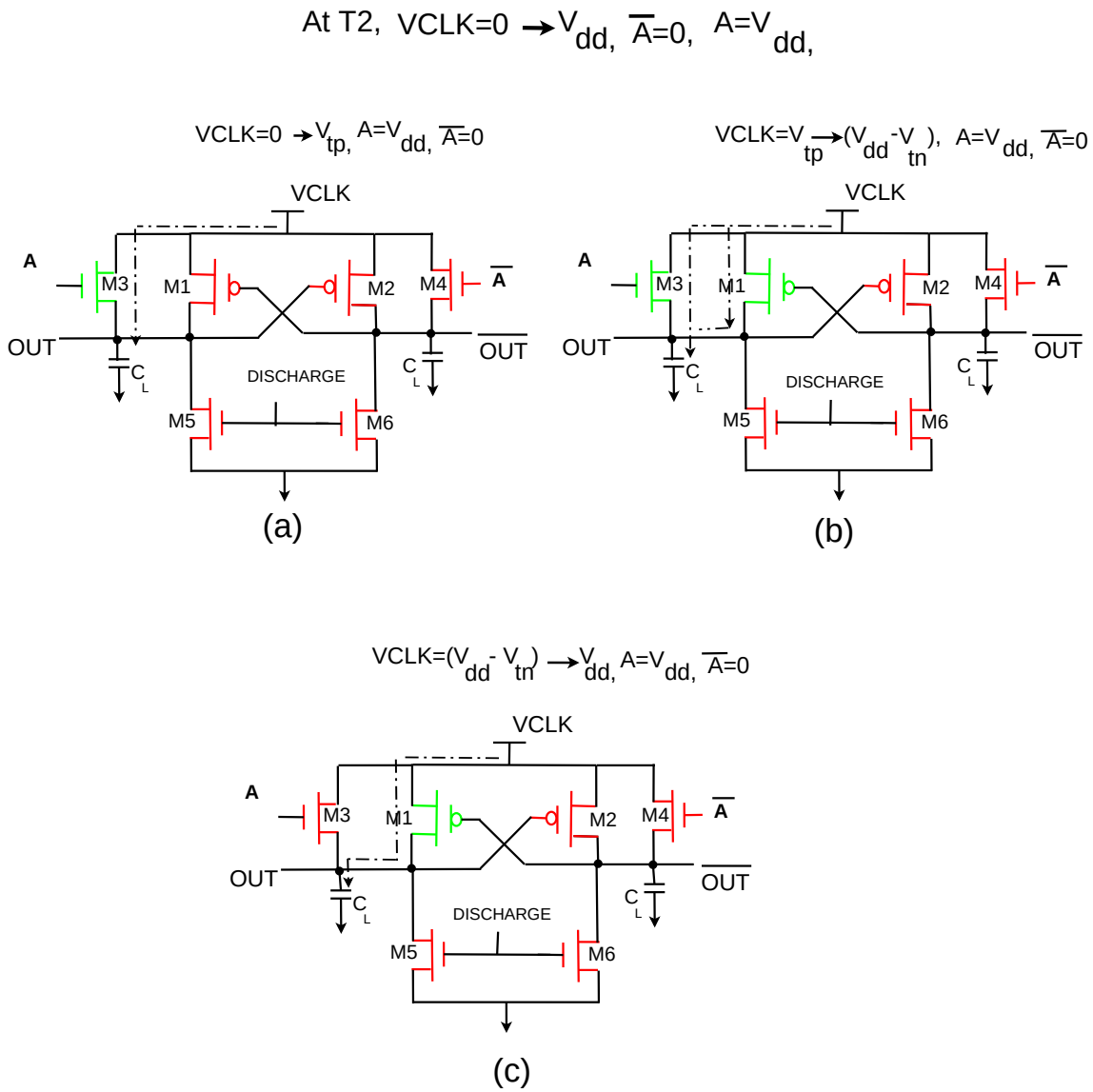


Figure 3.4: Switching operation of transistors in T2 phase of SPGAL buffer for A=1, $\bar{A}$=0. (a) represents the switching operation of the transistors when VCLK reaches V_{tp} from GND. (b) represents the switching operations when VCLK reaches from V_{tp} to $V_{dd} - V_{tp}$. (c) represents the switching operations when VCLK reaches V_{dd} from $V_{dd} - V_{tn}$

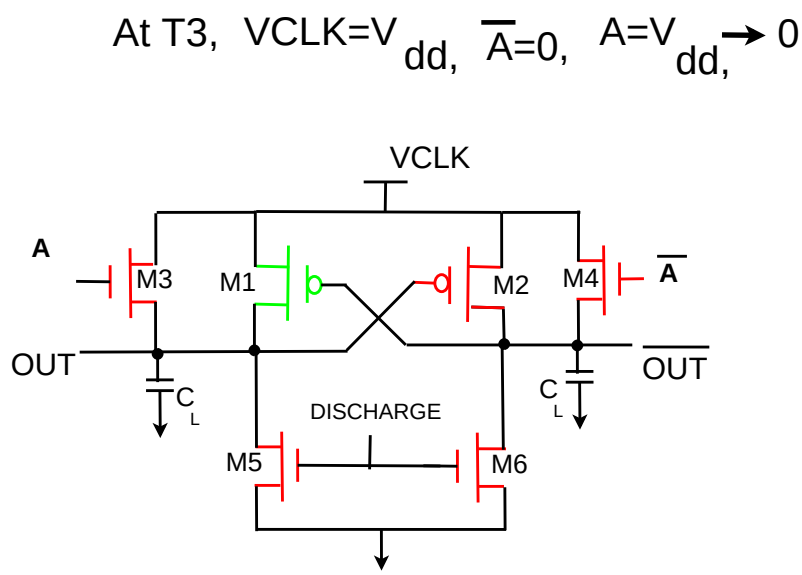


Figure 3.5: Switching operation of transistors in T3 phase of SPGAL buffer for A=1, $\bar{A}$=0

T3 (Hold Phase): At T3, the clock VCLK is at V_{dd}. The transistor M3 is turned off without non-adiabatic loss by slowly decreasing the inputs from V_{dd} to GND. The output will be same as T2 in this phase. Fig. 3.5 shows the switching operation of the transistors in T3 phase.

T4 (Recovery Phase): At T4, the clock VCLK slowly decreases from V_{dd} to GND. The charges stored in the output load capacitor is slowly recovered back to the clock through M1. Recovering of charge to the clock VCLK continues until OUT node reaches V_{t_p}.

$$V_{s_{M1}} - V_{G_{M1}} < V_{t_p}$$

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

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

When the output voltage is reduced to V_{tp}, M1 is turned off and the output voltage will stay at V_{tp} at the end of this phase. Fig. 3.6 shows the switching operation of the transistors in T4 phase. Charges stored in the output node at the end of the 1st

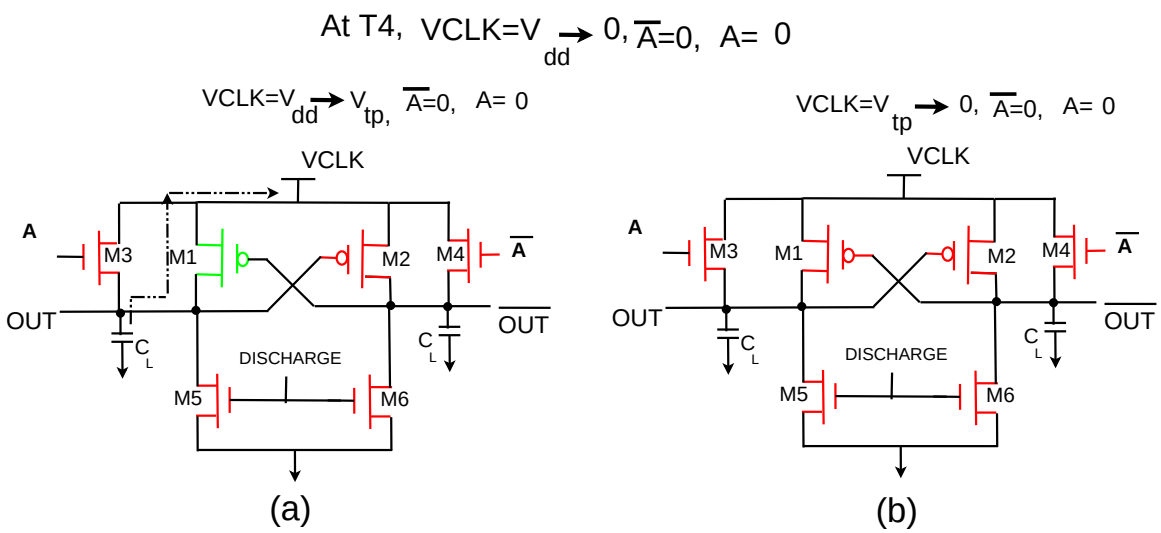


Figure 3.6: Switching operation of transistors in T4 phase of SPGAL buffer for A=1, $\bar{A}$=0. (a) represents the switching operation of the transistors when VCLK reach V_{tp} from V_{dd}. (b) represents the switching operation of the transistors when VCLK reach GND from V_{tp} .

cycle (T1-T4) is discharged to the ground in the next phase of the clock (T5) through M5 or M6 transistor by using the discharge signal. Resetting the output node to zero reduces the correlation between the current supplied and the data evaluated.

3.1.2 SPGAL XOR gate

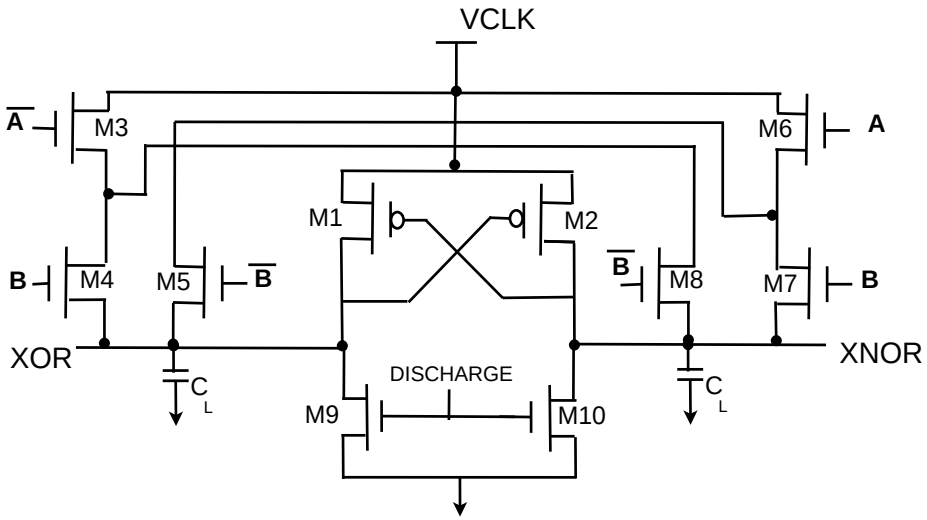


Figure 3.7: Proposed XOR/XNOR gate

This section covers the design of the proposed XOR gate. Fig. 3.7 shows the proposed XOR/XNOR gate. M1 and M2 forms the cross coupled structure to recover the charge stored in the output load capacitances. M9 and M10 transistors are used to reset the output nodes to zero by discharging the redundant charge stored in the load capacitances to ground. The rest of the transistors are used for evaluating the input data. The functionality of the proposed XOR/XNOR gate can be understood similar to the buffer as explained above. Fig. 3.8 shows the transient waveforms of the SPGAL based XOR gate. The instantaneous power plot of the proposed XOR gate for input transitions $(A, B) = (0, 0)(0, 1)(1, 0)(1, 1)(0, 0)$ is shown in Fig. 3.9. From Fig. 3.9, it can be seen that the SPGAL based XOR gate consumes uniform power for various transition of the inputs. The uniform instantaneous power show that the circuits built using the SPGAL based XOR gate can counteract the DPA attack at the circuit level. Fig. 3.10 shows the uniform supply current waveforms of the SPGAL based XOR gate.

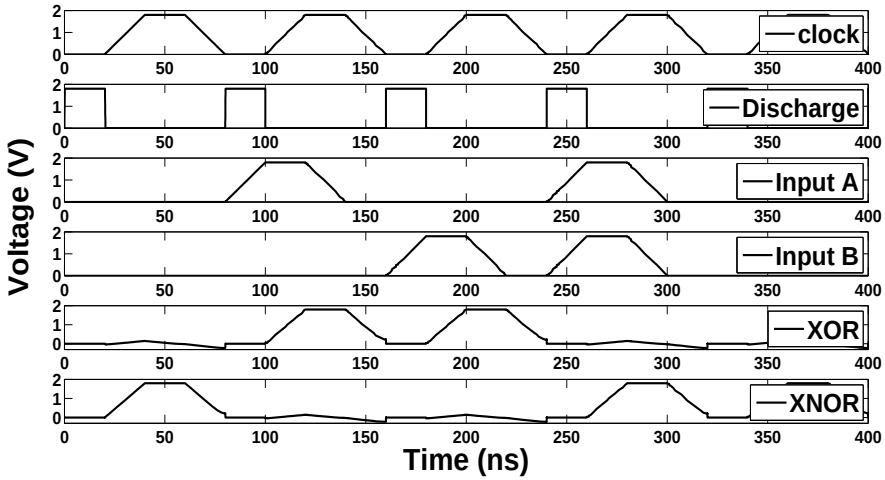


Figure 3.8: Input/output waveforms for the proposed XOR/XNOR gate

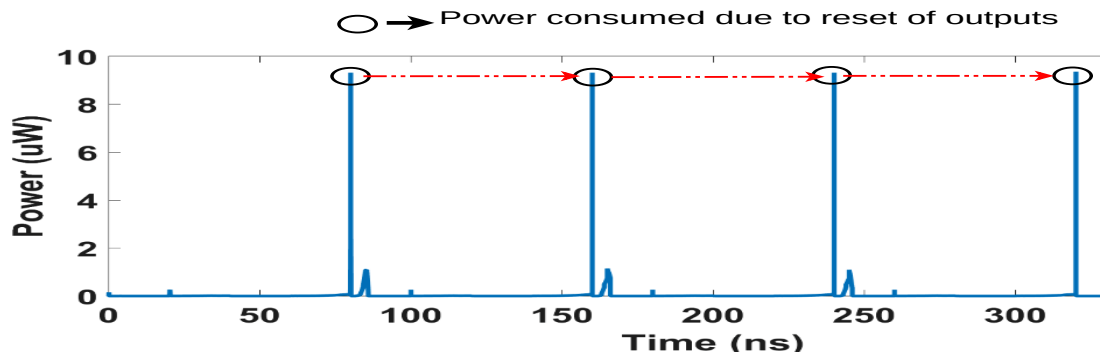


Figure 3.9: Power consumed by proposed XOR gate for input 00 → 01 → 10 → 11 → 00

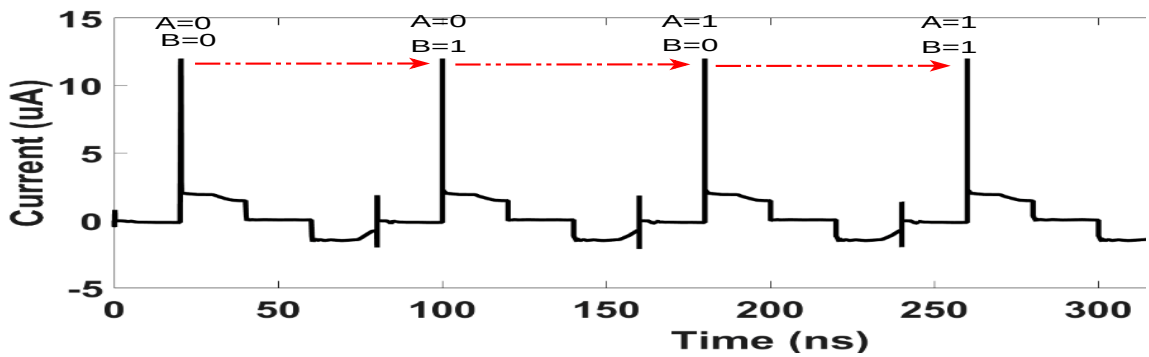


Figure 3.10: Supply current waveforms for various input transitions for proposed XOR gate

3.1.3 SPGAL AND gate

This section shows the design of the proposed AND gate in the Fig. 3.11 and the input/output waveforms in the Fig. 3.12

3.1.4 Simulation results

The proposed gates are simulated in 180nm technology with the load capacitance of 10fF. The simulation results of the individual logic gates are summarized in Table 3.1 and Table 3.2. The parameter Normalized Energy Deviation (NED) is defined as $(E_{max} - E_{min})/E_{max}$ is used to indicate the percentage difference between minimum and maximum energy consumption for all possible input transitions. Normalized Standard Deviation which was introduced by Bucci et.al[26] indicates the energy

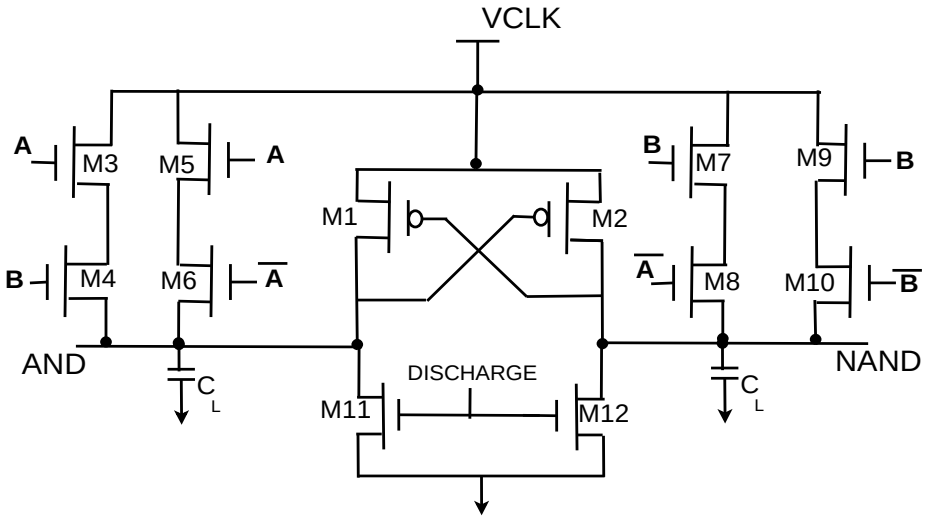


Figure 3.11: Proposed AND/NAND gate

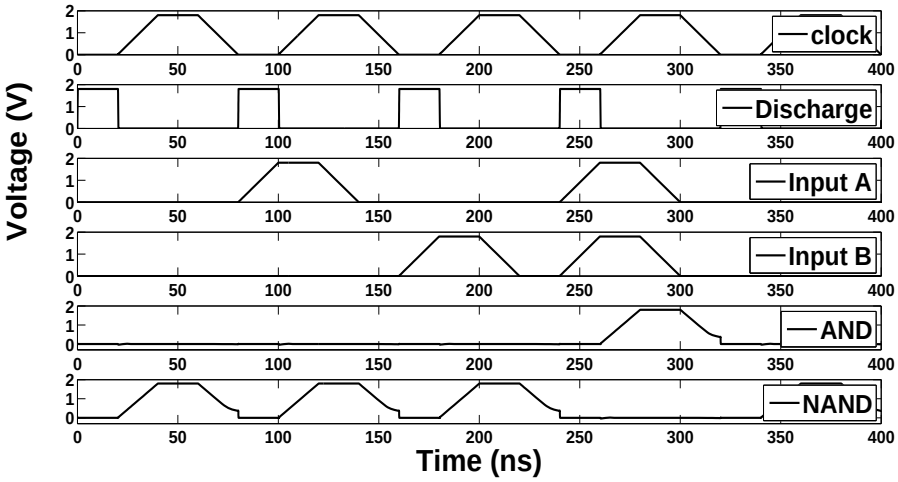


Figure 3.12: Input/output waveforms for proposed AND/NAND gate

consumption variation based on the inputs and it is calculated as $\frac{\sigma_E}{\bar{E}}$. $\bar{\mathrm{E}}$ denotes the average energy dissipation for various input transitions. In general, 'n' input gate will have 2^{2n} possible input transitions. For example, 2 input gate will have 16 input transitions. σ_E denotes the standard deviation of the energy consumed dissipated by the circuit and it is shown as $\sqrt{\frac{\sum_{i=E_1}^{E_n}(E_i-\bar{E})^2}{n}}$. The calculated values of NED and NSD for the proposed XOR gate and AND gate show the ability of the proposed logic family to resist DPA attacks. Apart from the logical ability, it has also been shown that

Table 3.1: Simulation and calculation results of AND logic gate for various DPA resistant adiabatic families

Logic family	**CSSAL[22]**			**SQAL[25]**			**SPGAL**		
Frequency(MHz)	1.25	12.5	125	1.25	12.5	125	1.25	12.5	125
E_{min}(fJ)	19.76	21.45	16.65	11.89	19.02	44.70	3.34	4.23	11.08
E_{max}(fJ)	20.07	21.70	21.47	12.66	24.93	53.69	3.75	4.66	11.66
E_{avg}(fJ)	19.92	21.59	19.48	12.26	21.93	49.08	3.56	4.43	11.40
SD (fJ)	0.08	0.09	1.48	0.25	2.07	3.10	0.12	0.14	0.16
NED%	1.39	1.15	22.45	0.06	0.23	0.16	0.10	0.09	0.04
NSD%	0.44	0.42	7.59	0.02	0.09	0.06	0.03	0.03	0.01

Table 3.2: Simulation and calculation results of XOR logic gate for various DPA resistant adiabatic families

Logic family	**CSSAL[22]**			**SQAL[25]**			**SPGAL**		
Frequency(MHz)	1.25	12.5	125	1.25	12.5	125	1.25	12.5	125
E_{min}(fJ)	19.80	21.59	16.65	9.20	13.85	30.48	1.80	1.86	6.83
E_{max}(fJ)	20.09	21.79	19.84	9.22	13.95	30.41	1.81	1.89	6.87
E_{avg}(fJ)	19.92	21.68	18.87	9.21	13.85	30.44	1.81	1.87	6.85
SD (fJ)	0.10	0.07	1.29	0.01	0.02	0.01	0.009	0.01	0.02
NED%	1.38	0.92	16.09	0.002	0.007	0.002	0.01	0.016	0.006
NSD%	0.52	0.32	6.86	0.001	0.001	0.005	0.005	0.008	0.003

the proposed logic consumes less power as compared to all the other DPA-resistant adiabatic circuits. The proposed logic gates are simulated in Cadence virtuoso using $180nm$ technology. The proposed logic gates have been used to implement bit-parallel cellular multiplier over $GF(2^m)$.

3.2 Implementation of bit parallel multiplier over $GF(2^m)$ using SPGAL gates

3.2.1 Galois Field Arithmetic

Finite field or Galois field plays a very important role in the field of cryptography [27]. It is used in the modern cryptographic algorithms such as AES [28]. Galois Field is identified with the following notation $GF(p^m)$, where p is a prime number and m is a

positive number. In $GF(p^m)$, p=2 is attractive for hardware circuit design using finite field multipliers. It is attractive because $GF(2)$ can be represented by the signals 0 and 1 [29]. $GF(2^m)$ contains 2^m elements which is an extension field of $GF(2)$. The finite field contains a zero element, an unit element, a primitive element and have at least one primitive irreducible polynomial $p(x) = x^m + p_{m-1}x^{m-1} + ... + p_1 + p_0$ over $GF(2)$ associated with it. The polynomial $p(x)$ is called as all one polynomial (AOP) of degree m if $p_i = 1$ for $i = 0, 1, 2, ...$ [30].

3.2.2 Bit-parallel multiplier

Let α be a root of irreducible AOP of degree m over $GF(2)$. Let us assume that $A = A_0 + A_1\alpha + A_2\alpha^2 + ... + A_m\alpha^m$. Let $B = B_0 + B_1\alpha + B_2\alpha^2 + ... + B_m\alpha^m$. Here, the element A and B are represented with the extended basis of $1, \alpha, \alpha^2, .., \alpha^m$. The product of multiplication A and B over $GF(2^m)$ is given by [31]:

$$AB = \Sigma_{i=0}^{m}\Sigma_{j=0}^{m}A_{<i-j>}B_j\alpha^i \tag{3.4}$$

For m=4, $A = A_0+A_1\alpha+A_2\alpha^2+A_3\alpha^3+A_4\alpha^4$, $B = B_0+B_1\alpha+B_2\alpha^2+B_3\alpha^3+B_4\alpha^4$ are the elements of $GF(2^4)$. The product of the multiplication of A and B over $GF(2^4)$ is denoted by $C = C_0 + C_1\alpha + C_2\alpha^2 + C_3\alpha^3 + C_4\alpha^4$. We can write

$$C_0 = A_0B_0 + A_4B_1 + A_3B_2 + A_2B_3 + A_1B_4$$

$$C_1 = A_1B_0 + A_0B_1 + A_4B_2 + A_3B_3 + A_2B_4$$

$$C_2 = A_2B_0 + A_1B_1 + A_0B_2 + A_4B_3 + A_3B_4$$

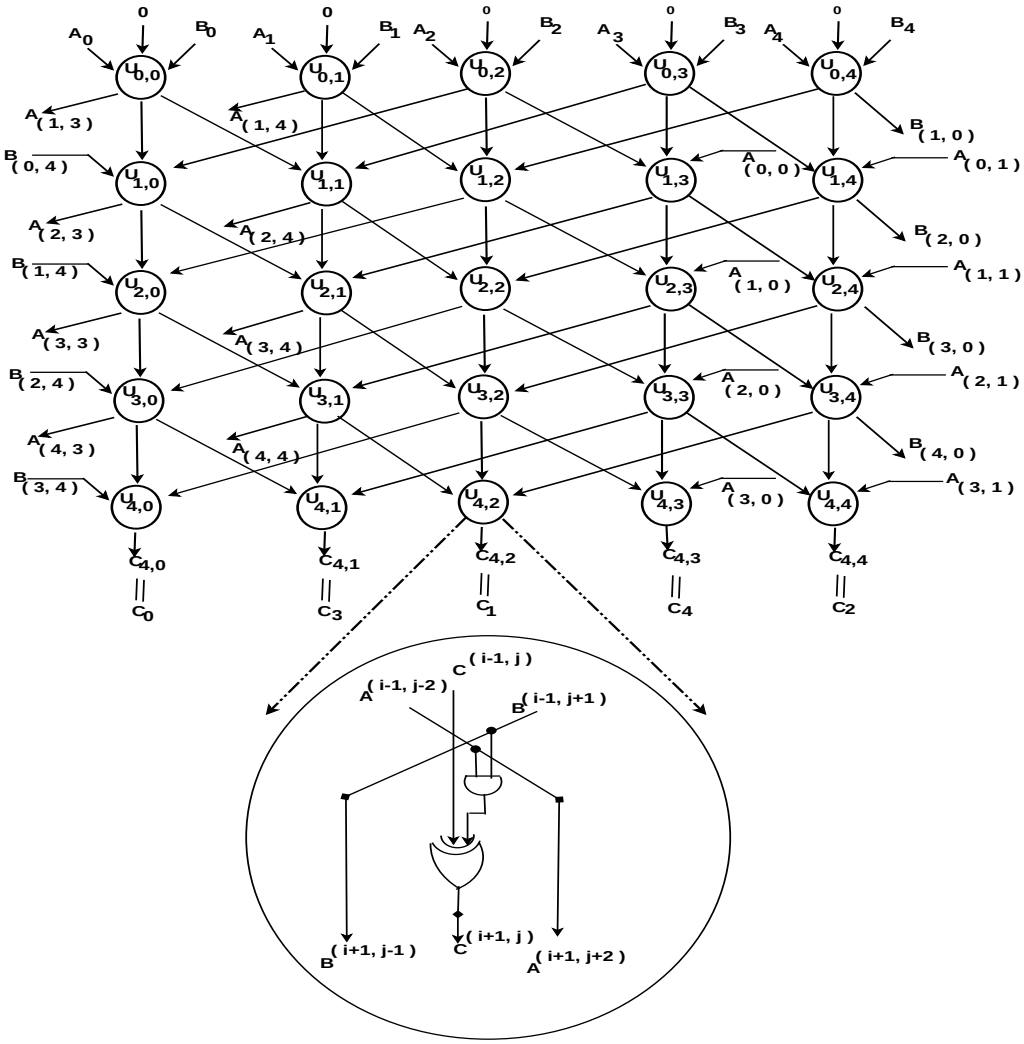
$$C_3 = A_3B_0 + A_2B_1 + A_1B_2 + A_0B_3 + A_4B_4$$

$$C_4 = A_4B_0 + A_3B_1 + A_2B_2 + A_1B_3 + A_0B_4$$

In the equations + denote the logic XOR operation and . denote the logic AND operation. We have used the proposed logic gates to implement the bit-parallel multiplier [2] which is low complex design ($(m+1)^2$ cells) with shorter computation time of $(m+1)(Tand + Txor)$, used for multiplication in $GF(2^m)$ and SPICE simulations have been done at different frequencies to verify its functionality. The architecture bit-parallel cellular multiplier is shown in Fig. 3.13. The clock supply and the discharge signal are shifted for each row of cells. If $A_0 = A_1 = A_2 = A_3 = A_4 = 1$ and $B_0 = B_1 = B_2 = B_3 = B_4 = 1$, then $C_0 = C_1 = C_2 = C_3 = C_4 = 1$. If $A_0 = A_2 = A_4 = 0$, $A_1 = A_3 = 1$, $B_0 = B_2 = B_4 = 1$, $B_1 = B_3 = 1$, $C_0 = C_1 = C_2 = C_3 = C_4 = 0$.

3.2.3 Simulation results

SPICE simulations are performed with $180nm$ technology library with the load capacitance of 10fF. The length and the width for both PMOS and NMOS transistors are $180nm$ and $600nm$ respectively. The Input and Output waveforms of bit-parallel cellular multiplier over $GF(2^4)$ implemented using SPGAL gates is shown in Fig. 3.14 and Fig. 3.15 respectively. Fig. 3.17 shows the supply current waveforms for the bit-parallel multiplier over $GF(2^4)$ implemented using SPGAL gates respectively. From Fig. 3.17, it can be inferred that the proposed gates when implemented in complex architecture will have uniform supply current waveforms. The transitional power dissipation is derived as E_{diss}=$\int_0^t V_{pc}(t)I_{pc}(t)$ where I_{pc} is the supply current waveforms and V_{pc} is the potential of the power clock. The results are observed at 12.5 MHz and compared with the existing DPA resistant adiabatic logic families. The energy dissipation of the proposed logic (0.556 pJ/cycle) is 90% less than the CSSAL logic (5.36 pJ/cycle) and 81% less than the SQAL logic (2.99 pJ/cycle). A plot comparing the energy dissipation per cycle of the bit-parallel cellular multiplier over $GF(2^4)$ designed with various DPA-resistant adiabatic families at different input frequencies



!h

Figure 3.13: Bit-parallel cellular multiplier for $GF(2^4)$ [2]

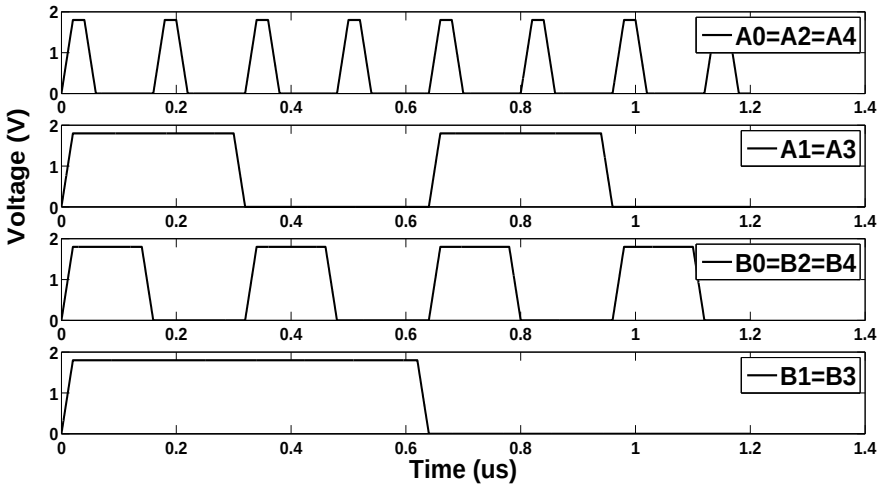


Figure 3.14: Input waveforms for the bit-parallel cellular multiplier over $GF(2^4)$

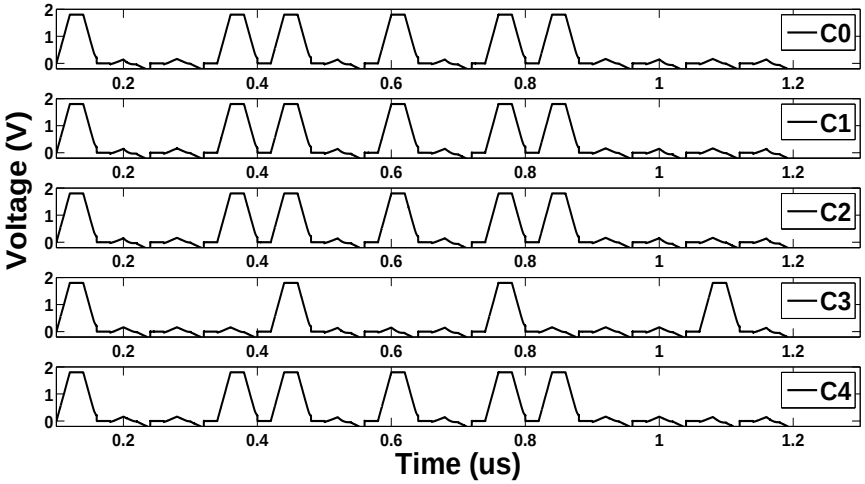


Figure 3.15: Output waveforms for the proposed logic based bit-parallel cellular multiplier over $GF(2^4)$

is shown in Fig. 3.16. It has to be noted that SAL logic in cellular multiplier over $GF(2^4)$ was not working at high frequencies. It is clearly seen from the plots that the multiplier designed with the proposed adiabatic family (SPGAL) dissipates less energy as compared to other DPA resistant adiabatic families.

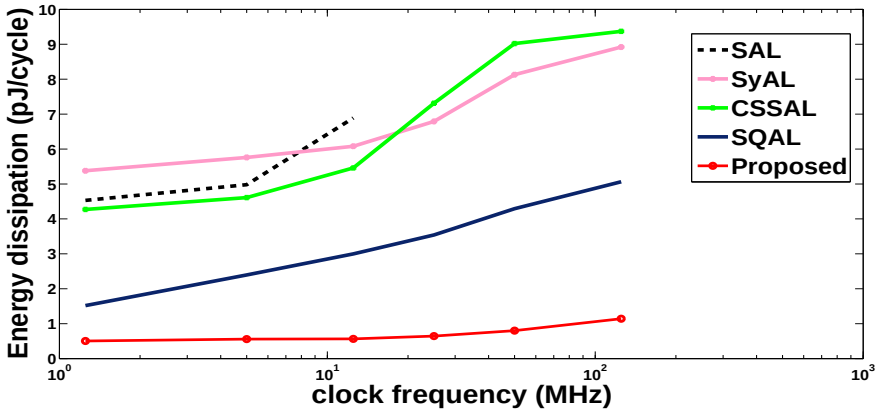


Figure 3.16: Energy dissipation comparison of the bit-parallel cellular multiplier over $GF(2^4)$ designed with various DPA resistant adiabatic families at different input frequencies.

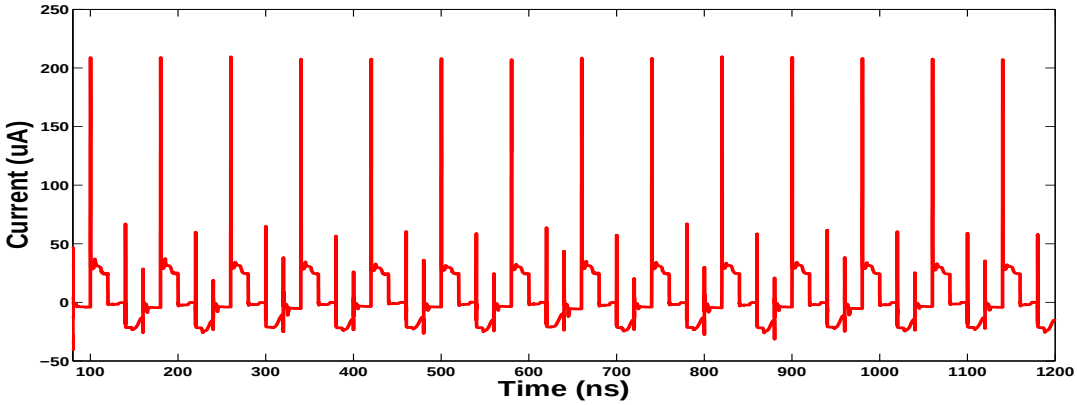


Figure 3.17: Supply current waveform for bit-parallel cellular multiplier over $GF(2^4)$ implemented using SPGAL gates

3.3 DPA attack on AES S-Box circuit implemented using SPGAL gates

3.3.1 Implementation of S-Box circuit

In the cryptographic algorithms such as AES/DES, S-Box is the key component for encryption/decryption operations. For example in an AES algorithm, four steps namely, SubBytes(bytesubstitution), ShiftRows,MixColumns and AddRoundKey are used to encrypt the data. Out of the four steps mentioned, SubBytes is the single

non-linear step in the AES algorithm where the input byte (8-bit) are replaced by the output of the S-Box circuit. In the AES algorithm, SubBytes operation is vulnerable to DPA attacks [32]. Fig. 3.18 represents the partial DPA attack on S-Box circuit. The internal circuit details of the S-Box architecture can be found in [33].

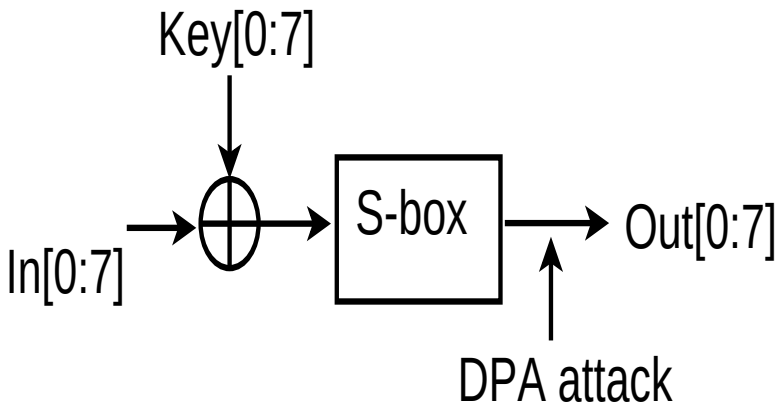


Figure 3.18: Partial DPA attack on 8 bit S-box circuit

Proposed SPGAL gates uses four phase trapezoidal clocks to recover the charges from the load capacitors. To build a complex structure using SPGAL, four trapezoidal clocks which have 90° phase shift with respect to its advance clock is employed. Note that in adiabatic circuits, the output of each gate is valid after one phase cycle of the clock. So, it is possible to connect the circuits in sequential manner. In the SBox circuit built using SPGAL and SQAL, buffers are inserted to synchronize the outputs of one stage and the other. For an adiabatic circuit with n-stages cascaded, the performance is similar to a pipeline circuit with n stages. In this case, SPGAL based S-Box circuit give the output with a delay of 5 clock cycles. Our SPGAL based S-box circuit is implemented in TSMC 180nm CMOS technology. The width and length of all the transistors used in the designs are 2um and 180nm respectively.

3.3.2 DPA attack

In order to evaluate the improvement produced by the SPGAL gates, three different S-Boxes were designed using 1) conventional CMOS, 2) SQAL, 3) proposed SPGAL gates. S-Boxes were designed in Cadence with 180nm technology. They are simulated in Spectre simulator with nominal conditions and T=27°C. The simulation environment was set up with a simulation resolution capturing data at every 1ns with a clock frequency 12.5 MHz. We have chosen to simulate the circuits at 12.5 MHz because SPGAL based gates are proposed to counteract DPA attacks for IoT devices. IoT based devices will work in low and medium frequencies. The simulations are done without any external noise source in order to ensure the best possible conditions for the attacker. The DPA attack is performed using the MATLAB after extracting the current traces from the Spectre simulator. We have used multi-bit correlation based DPA attack [34] to evaluate the security of SPGAL based S-box circuit. Figure 3.19 shows the DPA attack flow using the multi-bit correlation method.

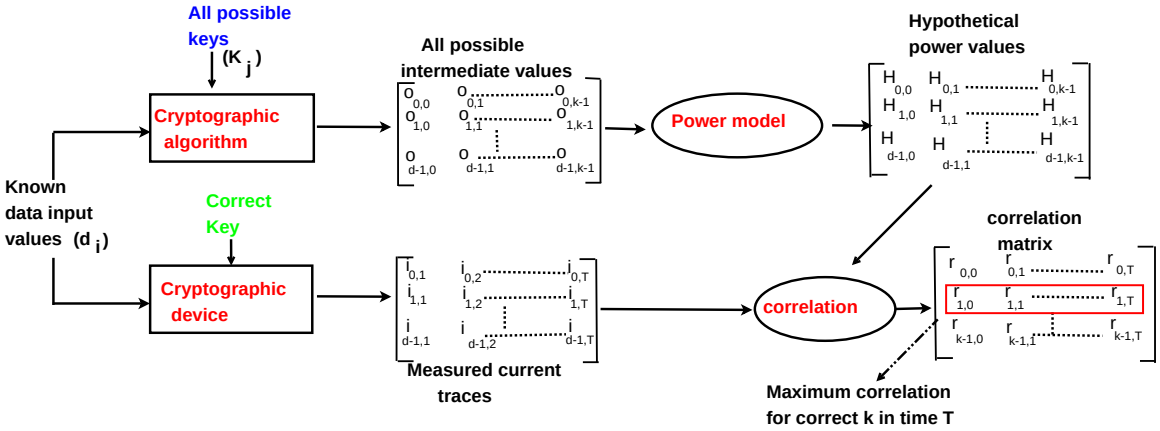


Figure 3.19: DPA attack flow using multi-bit correlation method

In our test case, DPA attack was performed with the key of $(181)_{10}$ and 512 random plain texts were passed to the 8-bit S-box circuit. Figure 3.20 shows the successful DPA attack in a conventional CMOS based S-box circuit. It has been shown that the correct key has the maximum correlation coefficient as compared to

the other key guesses. Figure 3.21 shows the unsuccessful DPA attack in a SPGAL based S-box circuit.

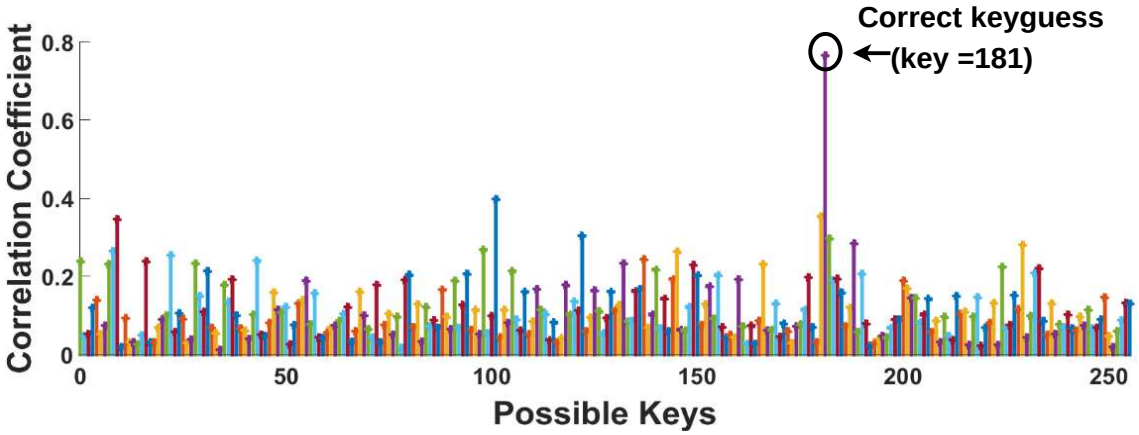


Figure 3.20: A successful DPA attack on CMOS based S-Box circuit

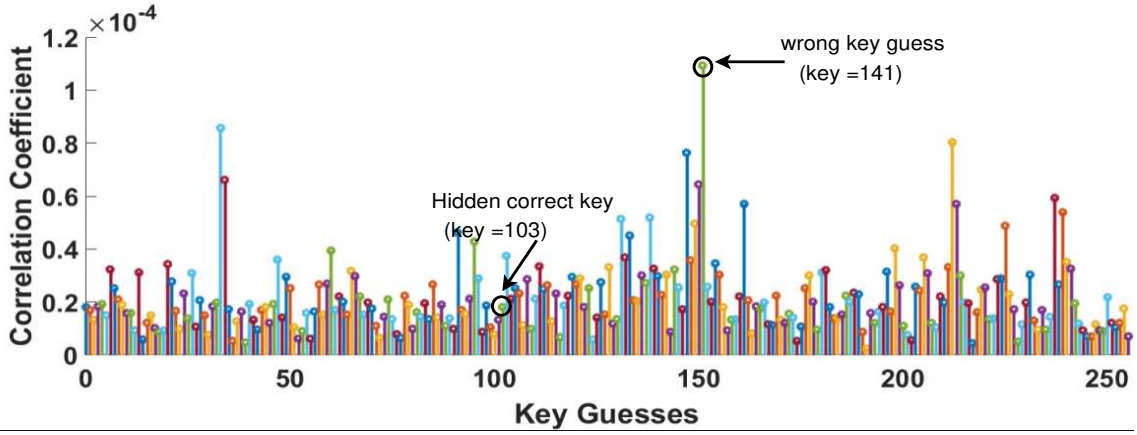


Figure 3.21: A unsuccessful DPA attack on SPGAL based S-Box circuit

3.3.3 Simulation results

We have compared all our results with the SQAL based adiabatic logic because SQAL shows better performance in terms of power consumption and area overhead as compared to the existing DPA-resistant adiabatic logic families. The transistor count and the energy dissipated per clock cycle of the SPGAL based S-Box circuit is compared with the conventional CMOS based S-Box circuit and SQAL based S-Box circuit.

Table ?? shows the comparison results of the SPGAL based S-Box circuit with the SQAL and conventional CMOS based S-Box circuit. we have used 135 XOR gates and 97 AND gates to implement the S-Box circuit. We have used 4 phase clocks to recover the charge stored in the load capacitor. So, additional buffers are used to synchronize the clocks from one stage of the S-Box circuit to the next stage. Since SPGAL and SQAL uses 4 phase clocks, both the logic requires 185 buffers to synchronize the clocks. Conventional CMOS logic requires 135 XOR gates and 97 AND gates to implement the S-Box circuit. Energy Saving Factor (ESF) values are shown in Table ??. Energy Saving Factor (ESF) is a measure of how much energy is used in a conventional CMOS gate or system with respect to its adiabatic logic counterpart [26].

Table 3.3: Comparison results

Logic	No. of Transistors	Overhead	Area (μ^2)	Energy diss/Cycle	ESF
CMOS	2202	-	0.04	11.45 pJ	-
SQAL [25]	3401	54%	0.0723	2.52 pJ	4.54
SPGAL	3624	64%	0.08	0.825 pJ	13.878

The area overhead of SPGAL and SQAL based S-Box circuit is 64% and 54% as compared to the S-Box circuit implemented using Conventional CMOS logic. Although the proposed SPGAL logic has the disadvantage in terms of transistor overhead, SPGAL shows a good improvement in terms of energy dissipation per clock cycle over SQAL and conventional CMOS logic. Proposed SPGAL based S-Box circuit dissipates 0.825 pJ of energy per clock cycle whereas SQAL based S-Box circuit and conventional CMOS based SBox circuit consumes 2.52 pJ and 11.45 pJ of energy per clock cycle respectively. It is clearly seen that the SPGAL based S-Box circuit saves up to 92% and 67% of energy as compared to the conventional CMOS and Secured Quasi-Adiabatic Logic (SQAL) based S-Box circuit. SPGAL and SQAL saves up to 92% and 78% of energy as compared to the conventional CMOS logic. The im-

provement in the energy dissipation makes SPGAL an interesting adiabatic logic to implement the secure IoT based devices. We have also simulated the SPGAL, SQAL and conventional CMOS based S Box circuits at different frequencies. It is clearly seen from the plot that the reduction of non-adiabatic loss in SPGAL family reduces the overall energy dissipation of the SPGAL based S-Box circuit at low and medium frequencies. Fig. 3.22 shows the energy dissipation comparison of the SPGAL, SQAL and conventional CMOS based S-Box circuits at different frequencies.

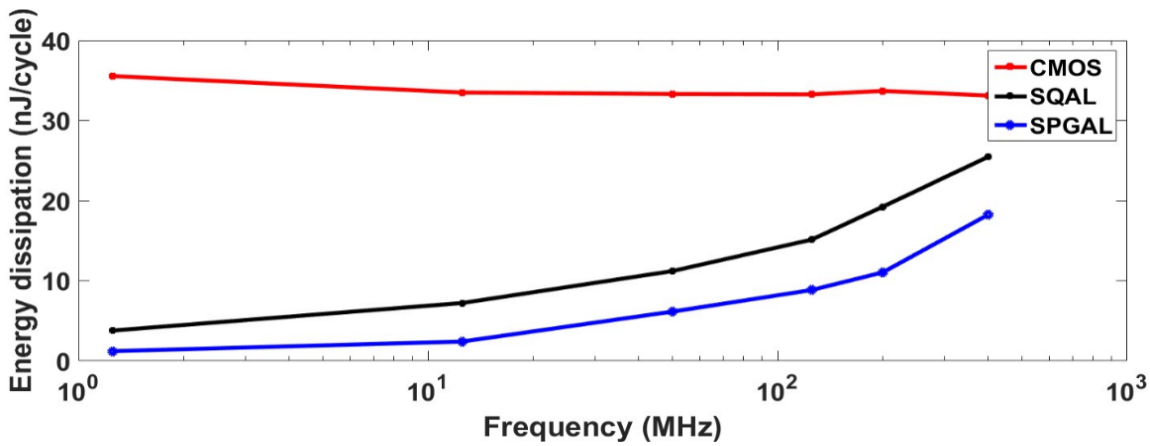


Figure 3.22: Energy dissipation comparison over different frequencies

3.4 CAD Automation

This section talks about the CAD scripts that were developed for automating large number of simulations which otherwise require time consuming manual effort to change the parameters of the simulation, run it and then perform power, delay calculations. The scripts were developed in ocean scripting language which is a derivative of SKILL language. SKILL language is developed by Cadence Design Systems. The scripts are written to calculate NED/NSD values of the circuits.

In general, a 'n' input gate will have 2^{2n} possible input transitions. For example, 2 input gate will have 16 input transitions as shown in Table 3.4. So that are 16 simulations to be run and energy calculations to be done to find out NED and NSD

values of a gate. This takes considerable amount of labor effort and time. Also a wrong change in the inputs will lead to incorrect results. The S-box circuit that was introduced in chapter 3 is an 8 input circuit, so there are 2^{16} input transitions. Running simulations manually does not make sense considering the amount of time it takes and little error margin. This was the motivation to develop scripts that do the simulations and calculations and provide with a final result conveniently.

Table 3.4: 2-Input Gate Input Transition Table

A	B	A	B
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

This script changes the input values, runs the simulation, calculates the Energy dissipation value and writes those values to a file. Next a post processor script parses through the file and generates the E_{max}, E_{min}, E_{avg} and σ values which are used to calculate NED/NSD values.

3.5 Conclusion

In this chapter we have proposed basic gates using adiabatic logic which show significant reduction in energy dissipation. Using these circuits, complex and larger designs were implemented and compared against circuits proposed in literature in terms of Energy Dissipation, NED and NSD. DPA attack was also performed on the AES S-Box creating using both CMOS and proposed SPGAL gates. The plots show that the proposed gates are resistant against such attacks. Also the motivation to develop automation scripts is discussed. These scripts reduce the amount of manual effort significantly eliminating the human error which can happen most likely because running the same simulation numerous times by changing the input pulse wave forms is highly susceptible to errors. These scripts not only run the simulations but also generate the required values to compare proposed designs against the designs proposed in literature, thus making it easy for us to work with CAD tools.

Chapter 4

Design of proposed Magnetic Tunnel Junction Circuits

A Logic-in-memory (LIM) paradigm can realize ultra-low-power architectures where memory elements are distributed over logic circuits [35] [36]. Further, LIM can reduce the delay of circuits by minimizing the long interconnection wires. Also, RAM based circuits have zero static power dissipation and they are very appropriate to achieve high performance and low-power designs [37]. Magnetic Tunnel Junction (MTJ) is a spin based device which is most suited to use in LIM architectures because of its short access time, small dimensions and compatibility with CMOS technology, etc. [38] [36][39][40][41].

In recent years, various hybrid MTJ/CMOS logic and arithmetic circuits such as magnetic full adder cell (MFA), magnetic flip-flop (MFF), magnetic look-up-table (MLUT) and magnetic content addressable memory (MCAM) have been proposed [36][42][43][44][16].

4.1 4-2 compressor circuit

A 4-2 compressor is a module which has five inputs (X1, X2, X3, X4 and Cin) and three outputs (Sum, Carry and Cout). The weights of the four inputs X1, X2, X3 and X4 and the sum output are same. The weight of the carry output is one binary bit higher than the four inputs and sum. The input to the 4-2 compressor is supplied from the Cin of the preceding module of one binary bit lower. The Cout of the compressor is supplied to the next compressor module of higher significance. The fundamental equation of the 4-2 compressor is given as [45]:

$$X1 + X2 + X3 + X4 + Cin = Sum + 2(Carry + Cout) \tag{4.1}$$

The conventional 4-2 compressor consists of two full adder cells as shown in Fig. **??**. In order to accelerate the carry-save summation of the partial products, it is important that carry output (Cout) is independent of carry input (Cin). The output functions of a 4-2 compressor are shown in equations 2-5.

$$Cout = X1.X2.\overline{X3} + X1.\overline{X2}.X3 + \overline{X1}.X2.X3 + X1.X2.X3 \tag{4.2}$$

$$S = X1 \oplus X2 \oplus X3 \tag{4.3}$$

$$Sum = S \oplus X4 \oplus Cin = X1 \oplus X2 \oplus X3 \oplus X4 \oplus Cin \tag{4.4}$$

$$Carry = (Cin \oplus X4).S + Cin.X4 \tag{4.5}$$

4.2 Proposed Hybrid MTJ/CMOS 4-2 compressor circuit

The proposed hybrid MTJ/CMOS 4-2 compressor circuit consists of three different modules namely, sum, carry and cout circuits. Fig. 4.1, Fig. 4.2 and Fig. 4.3

shows the schematics of the Cout, Sum and the Carry output of the proposed hybrid MTJ/CMOS 4-2 compressor. We have used the dynamic current mode method to design our circuits. The compressor's three modules (Cout, Sum and Carry) are designed based on the equations 4.2 - 4.5. For example, for designing Sum output a 5-input XOR has been implemented. Also to design the Carry module, we had to implement a 3-input XOR and AND gates based on equation 4.5. The following subsections discuss the functionality of each module of the proposed hybrid MTJ/CMOS 4-2 compressor. In this design, the value of the X3 input is stored in the MTJs.

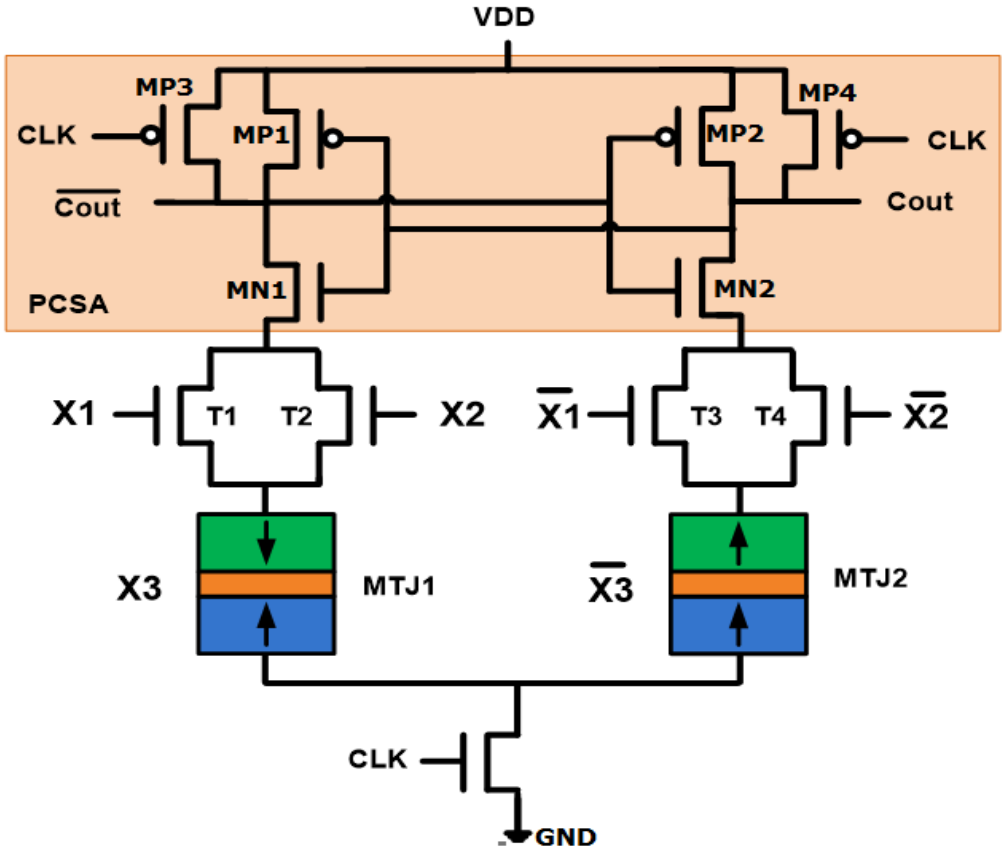


Figure 4.1: Schematic of the Cout output

4.2.1 Cout circuit

Fig. 4.1 shows the schematic of the Cout output of the proposed hybrid CMOS/MTJ 4-2 compressor. The design of the Cout module is much simpler than the design of the other two modules. Based on equation 2, this circuit is a majority gate and can be designed as a previously presented full adders carry output (Fig. 4.1) [38]. In this circuit, when both X1 and X2 are at VDD, T3 and T4 are OFF and the Cout output remains charged regardless of the X3 input. When both X1 and X2 are zero, T1 and T2 are OFF and Cout will be discharged to ground. If the input value stored in MTJ1 is "1" and MTJ2 is "0", then the state of MTJ1 and MTJ2 will be parallel and anti-parallel, respectively and Cout will be VDD. If X3 is zero, the state of MTJ1 and MTJ2 will remain in their initial states which were anti-parallel and parallel, respectively. Consequently, Cout will be discharged to the ground.

4.2.2 Sum circuit

The schematic of the Sum output circuit is shown in Fig. 4.2. Based on equation 4, The Sum output is a 5-input XOR. The initial states of MTJ1 and MTJ2 are antiparallel and parallel, respectively. When the input X3 is changed from zero to VDD, the MTJ states will be changed. This circuit implements a 5-input XOR and XNOR. As it can be seen from Fig. 4.2, the top parts of the pull down circuit are XOR (X4,Cin) and XNOR (X4,Cin) which are highlighted in the figure. In this circuit we implemented XORs and XNORs hierarchically. So the circuit is designed and implemented based on the following equation. Sum=X1.X2.X3.X4.Cin+X1.X2.X3.$\overline{X4}.\overline{Cin}$ + $X1.\overline{X2}.X3.X4.\overline{Cin}+\overline{X1}.X2.X3.X4.\overline{Cin}+\overline{X1}.X2.X3.\overline{X4}.Cin+X1.\overline{X2}.X3.\overline{X4}.Cin+X1.X2.\overline{X3}.\overline{X4}.Cin+X1.\overline{X2}.\overline{X3}.X4.Cin+\overline{X1}.X2.\overline{X3}.X4.Cin+\overline{X1}.X2.\overline{X3}.X4.Cin+\overline{X1}.\overline{X2}.X3.X4.Cin+\overline{X1}.\overline{X2}.\overline{X3}.\overline{X4}.Cin+\overline{X1}.\overline{X2}.\overline{X3}.X4.\overline{Cin}+\overline{X1}.\overline{X2}.X3.\overline{X4}.\overline{Cin}+\overline{X1}.X2.\overline{X3}.\overline{X4}.\overline{Cin}+X1.\overline{X2}.\overline{X3}.\overline{X4}.\overline{Cin}$

The proposed designs are based on precharge logic. So, when the CLK is in precharge

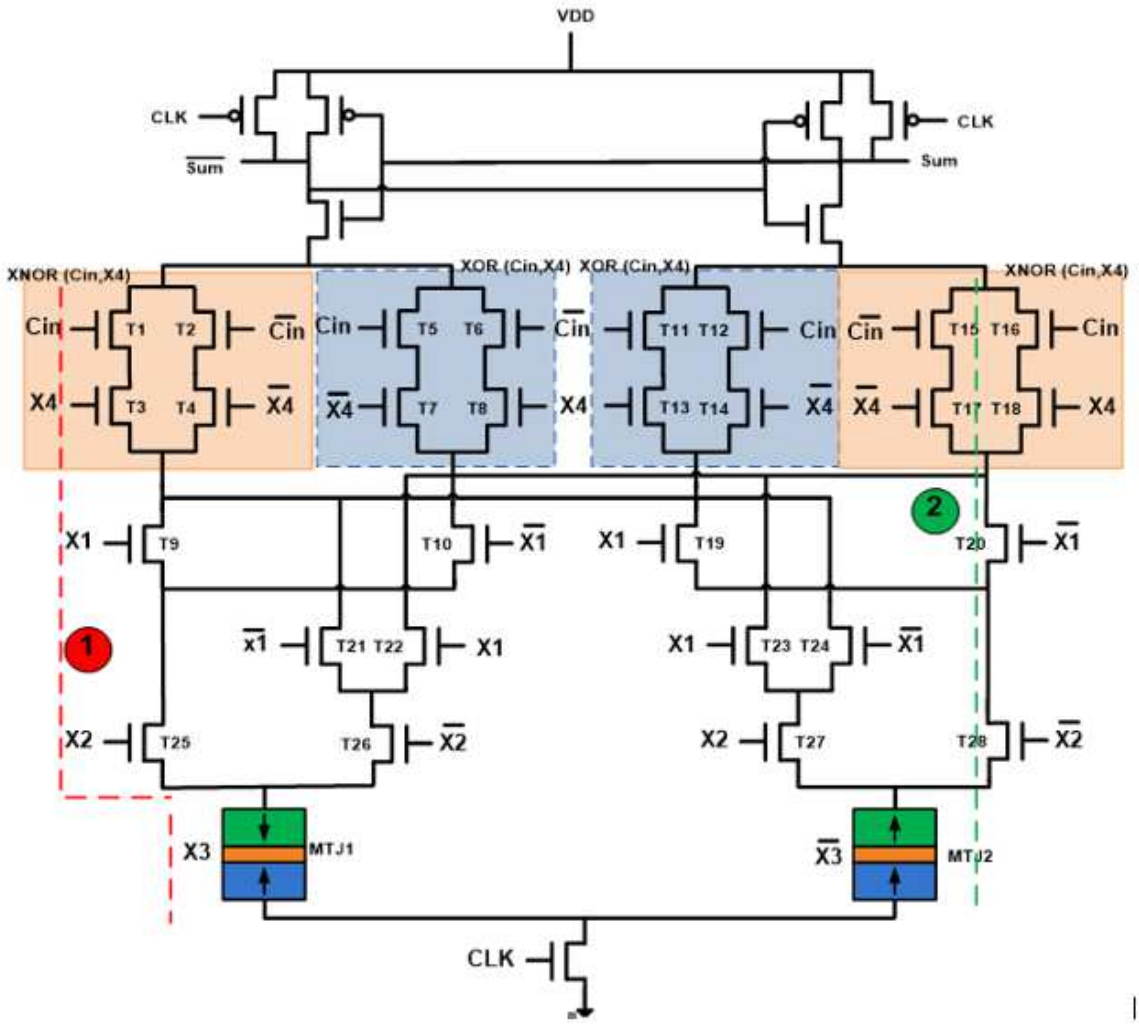


Figure 4.2: Schematic of the Sum output. Paths 1 and 2 indicate the discharge paths for patterns 11111 and 00000 for $\overline{Sum}$ and Sum outputs respectively (Red and Green paths)

phase (CLK=0), all the output nodes will be precharged to VDD. Let us assume that the input for the sum circuit is 00000. With this input pattern, the Sum output will be discharged through T15, T17, T20, T28 and MTJ2 which is shown with path 2 in Fig. 4.2. When the input pattern is 11111, $\overline{Sum}$ will be discharged through transistors T1,T3,T9, T25 and MTJ1(path 1) and consequently Sum will be VDD. If the input pattern is 10111, the Sum output will be discharged by T16, T18, T22, T26 and MTJ1 and thus we have zero at this output. For other input patterns, the outputs will either remain charged or be discharged similarly based on the input patterns.

4.2.3 Carry circuit

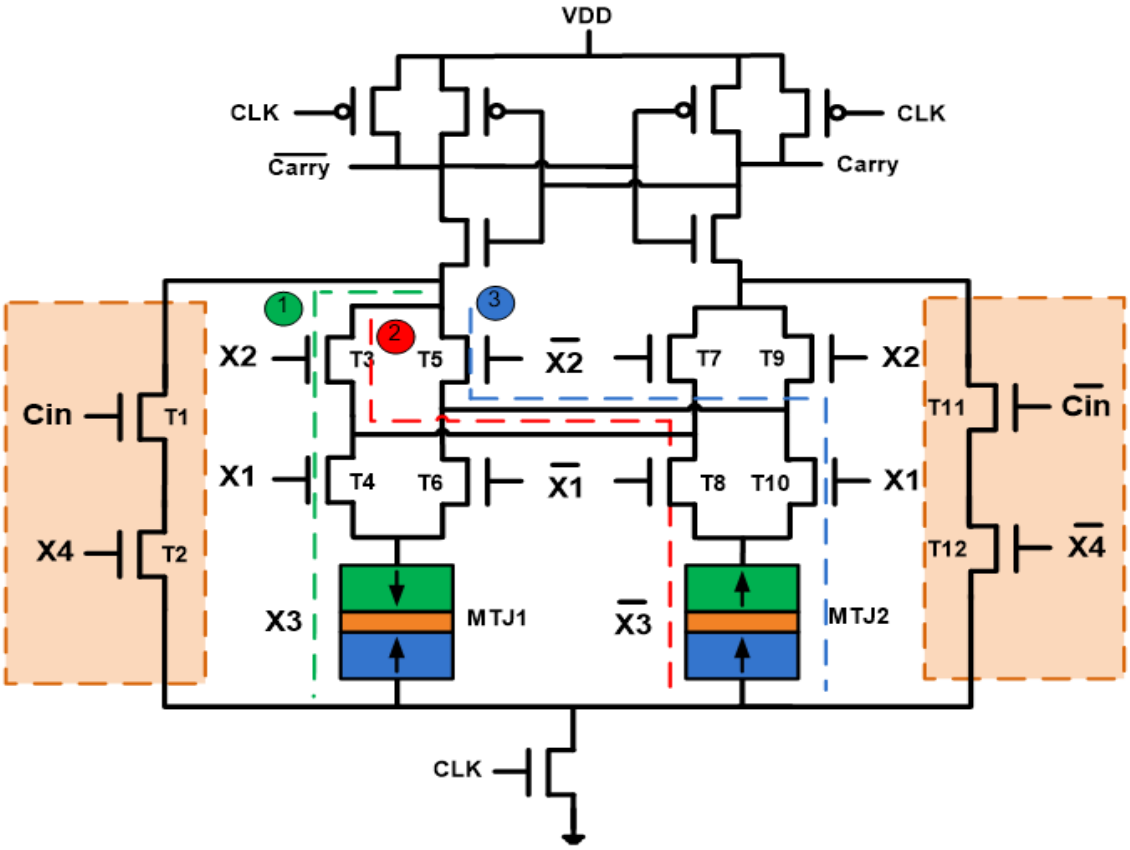


Figure 4.3: Schematic of the Carry output. Paths 1, 2 and 3 implement the XOR function

The last part of the proposed 4-2 compressor is the carry generator circuit (Fig. 4.3). According to equation 4.5, when X4 and Cin are both VDD the output is VDD. Also, when these signals are both zero the output will be zero. If we have 01 or 10 for X4Cin, the output will be determined based on the XOR of the other three inputs. As shown in Fig. 4.3, when X4 and Cin are given VDD, the leftmost path (T1 and T2) will discharge the $\overline{Carry}$ signal to the ground. If X4 and Cin are both zero, the rightmost path (T11 and T12) will discharge the Carry signal to the ground and we have zero at the output. In other cases, the Carry output will be discharged and remain charged by the XOR and XNOR circuits which are implemented in the middle of Fig. 4.3. Based on equation 5, when X4 and Cin have the same value the

Carry output will be determined by the output of XOR (X1,X2,X3). This function can be calculated through the paths 1, 2 and 3 shown in Fig. 4.3. Path 1 gives the X1X2X3, path 2 gives $\overline{X1}X2\overline{X3}$ and path 3 implements $X1\overline{X2X3}$ minterms. For example, when the input pattern is 10101 for X1X2X3X4Cin the left and right paths are disconnected and the Carry will be discharged through T7, T4 and MTJ1. The resulting output will be zero. For all of the designs, the write circuits are similar to the previous presented paper [16]. Fig. 4.4 shows the transient response of the proposed 4-2 compressor.

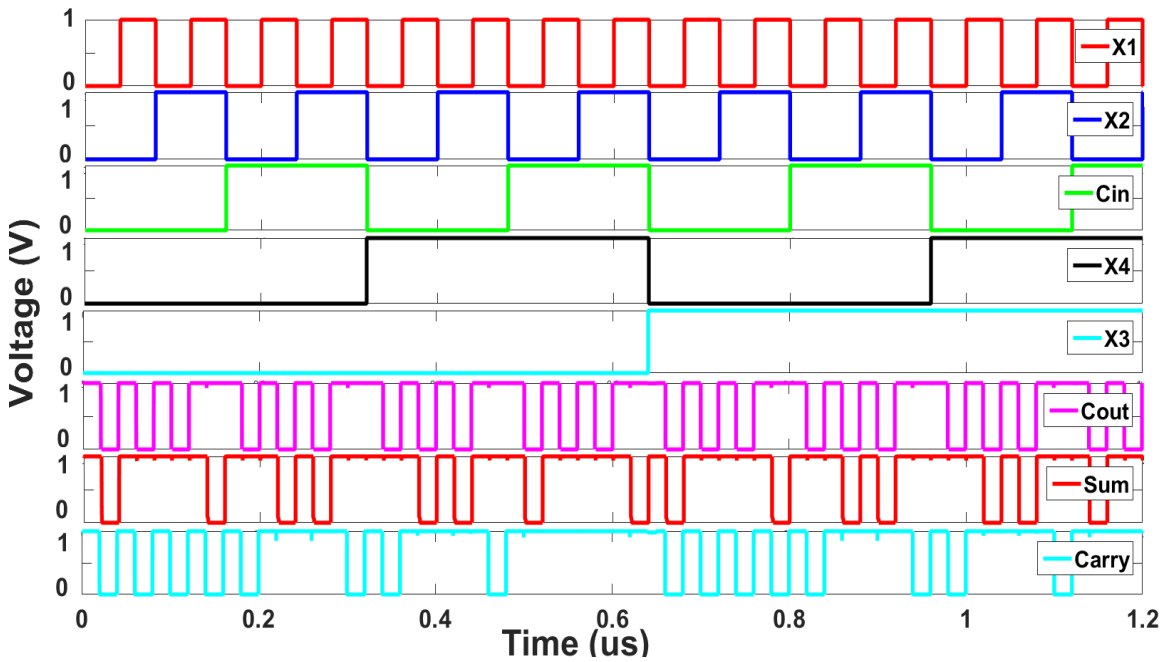


Figure 4.4: Transient response of the proposed 4-2 compressor

4.2.4 Simulation results

MTJ device parameters which are used for simulation done in Cadence Virtuoso are given in Table 4.1. The library used was 45nm library. Table 4.2 shows the Power delay Product (PDP) comparison between the proposed 4-2 compressor circuit and circuits proposed in [46][45].

Table 4.1: MTJ device parameters used for simulations

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

Table 4.2: Simulation results with 45nm technology

Design	Delay (ps)	power (μW)	PDP (10^{-18}J)
Design [45]	83.2	0.103	8.5696
Design [46]	80.2	0.122	9.784
Proposed	66.7	0.085	5.67

Table 4.3 represents the delay, power consumption and PDP of circuits in 0.9V supply voltage and 1fF load capacitor with 32nm technology. The proposed MTJ/CNFET design has better results in all evaluation criteria compared to the CMOS based circuits.

Table 4.3: Simulation results with 32nm technology

Design	Delay (ps)	power (μW)	PDP (10^{-18}J)
Design [45]	112	0.09	10.08
Design [46]	94.4	0.12	11.38
Proposed/CMOS	71.2	0.08	5.6
Proposed/CNFET	26.8	0.01	2.6

Fig. 4.5 shows the PDP variation with respect to change in Voltage, Temperature and Threshold Voltage.

4.3 Hybrid CNFET/CMOS 4-2 compressor circuit

We utilized CNFETs in the proposed 4-2 compressor structure and implemented the hybrid MTJ/CNFET 4-2 compressor as shown in the figure 4.6. We have used the

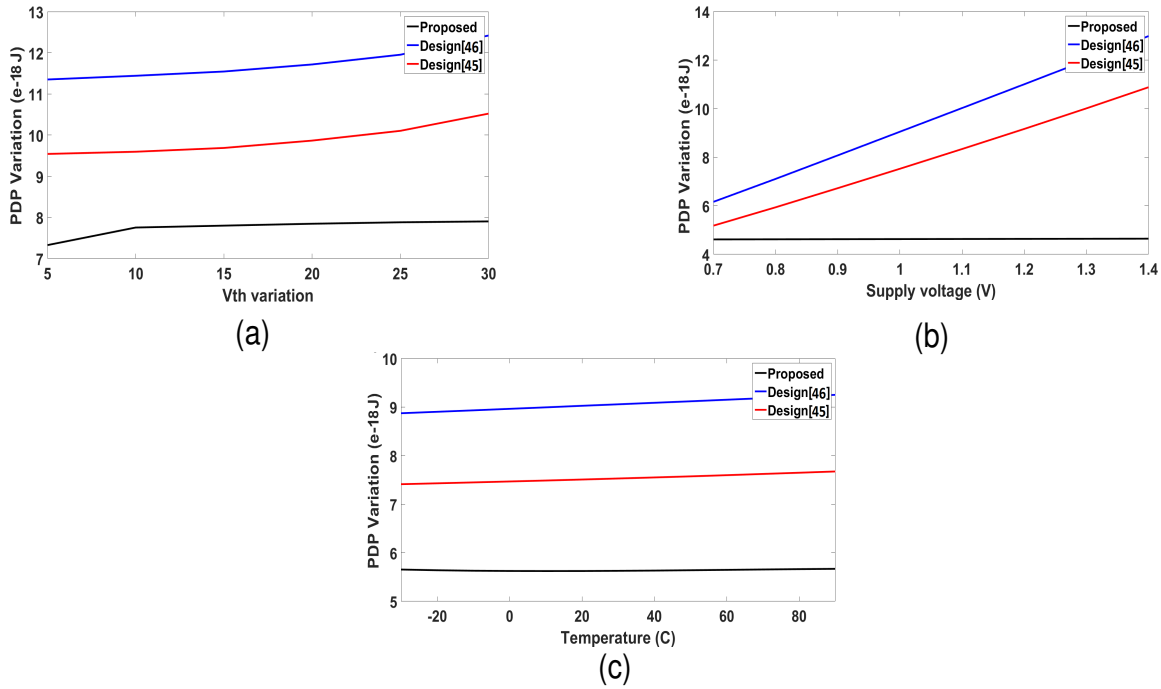


Figure 4.5: Power-Delay Product (PDP) comparison of 4-2 compressor with Process, Voltage, Temperature (PVT) variations

compact SPICE model for unipolar MOSFET-like CNTFET including all the non-idealities, parasitics and quantum effects [47] for simulating CNFET/MTJ circuit. Fig 4.7 shows the transient waveforms for the cascaded 4-2 compressor.

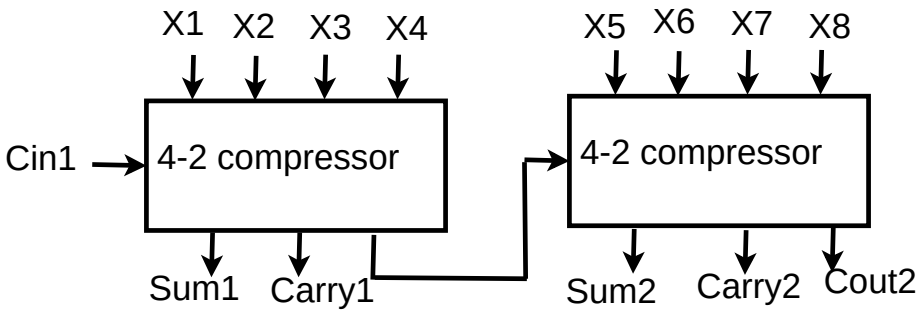


Figure 4.6: Structure of cascaded 4-2 compressor

4.3.1 Simulation results

Table 4.4 shows the device parameters used for CNFET models in our simulations. Table 4.5 shows the simulation results of the cascaded 4-2 compressor. It is inferred

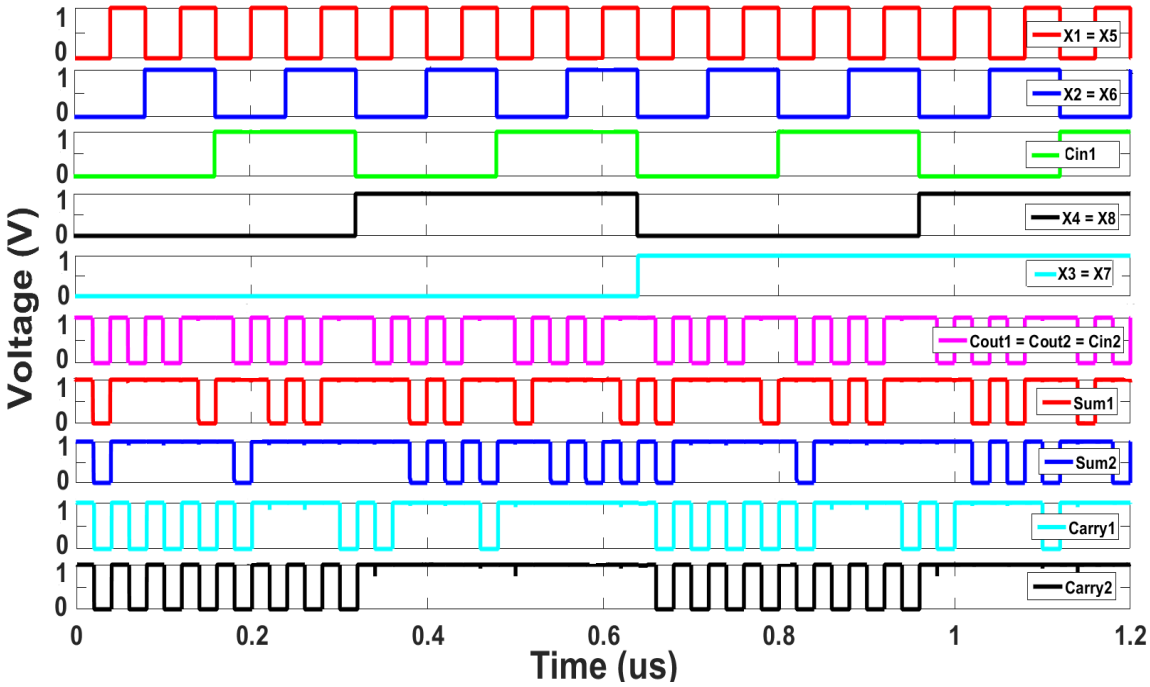


Figure 4.7: Transient waveform of cascaded 4-2 compressor

that the proposed MTJ/CNFET based cascaded 4-2 compressor has lower PDP as compared to the existing compressor designs.

Fig. 4.8 shows the PDP variation with respect to change in Voltage, Temperature and Threshold Voltage.

4.4 Conclusion

In this chapter we proposed a hybrid MTJ/CMOS 4-2 compressor circuit that reduces the energy consumption substantially by making use of the MTJ unique properties. We can see that the PDP is reduced by nearly 50%. This was further improved by replacing CMOS with CNFET.

Table 4.4: CNFET device parameters used for simulations

arameter	Description	Value
L_{ch}	Physical Channel Length	32nm
L_{geff}	The mean free path in the intrinsic CNT channel	100nm
L_{dd}	The length of doped CNT drain side extension region	32nm
L_{ss}	The length of doped CNT source side extension region	32nm
T_{ox}	The thickness of high-k-top gate dielectric material	1nm
K_{gate}	The dielectric constant of high-k-top gate dielectric material	16
E_{fi}	The Fermi level of doped S/D tube	6ev
C_{sub}	The coupling capacitor between the channel region and the substrate	20 pF/m

Table 4.5: Simulation results of cascaded 4-2 compressor

Design	Delay (ps)	power (μW)	PDP (10^{-16}J)
Design [45]	86.2	0.5	0.4
Design [46]	83.4	0.667	0.55
Proposed	69.2	0.42	0.29

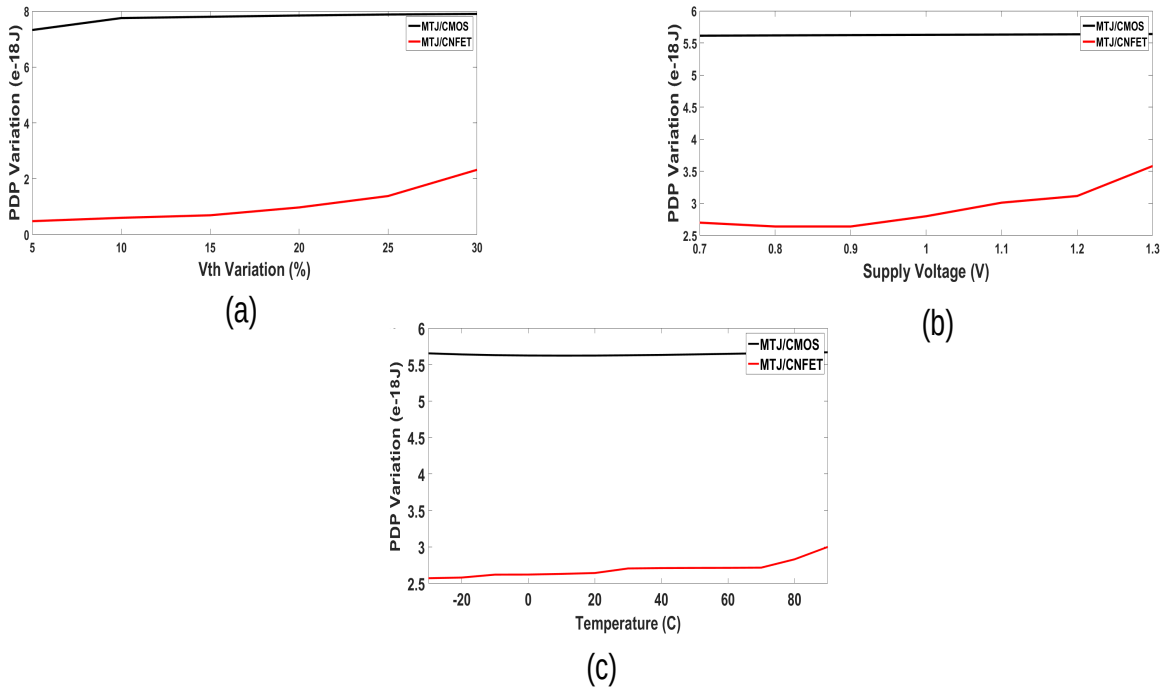


Figure 4.8: Comparison of CMOS/MTJ and CNFET/MTJ in term of PDP variation against PVT variation

Chapter 5

Conclusions

In this thesis, adiabatic paradigm was explored and a novel family of Adiabatic logic SPGAL was proposed. Using this proposed logic low power and DPA secure gates were designed. The applications of these circuits are apt for IoT devices since they operate at low frequencies and power constrained scenarios. At high frequencies (above 200 MHz) the same amount of energy is dissipated compared to circuits designed in CMOS logic which makes adiabatic logic not a feasible option. The adiabatic logic is also one of the techniques that removes the data and power dependency making it difficult for the attacker to find out the encryption key used in cryptographic processors. At the same time the energy that is dissipated is sent back to the clock generator, thus reducing the energy consumption significantly. From the simulation reports we can see that there is nearly 80% reduction in energy consumption when compared to CMOS. On a system level, if each gate is implemented using SPGAL gates, you can have atleast 70% - 80% energy savings. However these perks do come at a cost. The adiabatic family logic is dual rail in nature, thus this leads to an area overhead. The transistor count for even such a simple circuit like an buffer which takes only four transistors in CMOS logic takes six transistors to design. Not just this, the clock that is used in adiabatic logic is 4-phase trapezoidal clock. This makes

designing larger circuits difficult because synchronizing the signals will prove to be an ordeal. In order to synchronize them additional buffers have to be used leading to extra area for the chip. Moreover the EDA tools do not support this kind of phased clock distribution. Therefore this will be a manual and hectic work to have all the signals synchronized. Adding this kind of support in EDA tools will ease the chip designing effort tremendously, so this can be an area that people can focus on in future to benefit from the adiabatic logic.

The hybrid MTJ/CMOS circuits proposed in this thesis show a promising 50% reduction in Energy consumption. This was further improved by using CNFET in place of CMOS as the PDP was reduced by nearly 80%. Designing circuits using MTJ/CNFET is not as complex as designing with adiabatic logic since there is no synchronization of signals needed because all the gates operate on same clock signal. However using CNFET may pose challenge while manufacturing. Since its structure is not as simple as CMOS and the fabs currently do not have masks developed to lay out CNFETs on a massive scale. As of now the models are developed for MTJ/CNFETs which can be used only for the purpose of simulation. Although the models prove helpful to get an insight as to how using MTJ/CNFET will prove advantageous, they are still not perfect as current CAD tools do not support these models entirely. Energy calculations in the CAD tool generates incorrect values when done by using the inbuilt calculator. Also multiple writes to the MTJ cells do not seem to take effect. So, these are few problems which can be fixed so that any future work on MTJs does not seem tedious.

References

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

[2] LIU Chung-Hsin, Nen-Fu Huang, and LEE Chiou-Yng. Computation of ab 2 multiplier in gf (2 m) using an efficient low-complexity cellular architecture. *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, 83(12):2657–2663, 2000.

[3] An introduction to the internet of things (iot). `https://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf`.

[4] The statistics portal. (2017). internet of things (iot) connected devices installed base worldwide from 2015 to 2025 (in billions). `https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/`.

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

[6] Xueqing Li, Kaisheng Ma, Sumitha George, John Sampson, and Vijaykrishnan Narayanan. Enabling internet-of-things with opportunities brought by emerging devices, circuits and architectures. In *IFIP/IEEE International Conference on Very Large Scale Integration-System on a Chip*, pages 1–23. Springer, 2016.

[7] Pei-Yih Ting, Jia-Lun Tsai, and Tzong-Sun Wu. Signcryption method suitable for low-power iot devices in a wireless sensor network. *IEEE Systems Journal*, 12(3):2385–2394, 2018.

[8] PP Freitas, R Ferreira, S Cardoso, and F Cardoso. Magnetoresistive sensors. *Journal of Physics: Condensed Matter*, 19(16):165221, 2007.

[9] 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, the VLSI Journal*, 58:369–377, 2017.

[10] S Dinesh Kumar, Himanshu Thapliyal, Azhar Mohammad, Vijay Singh, and Kalyan S Perumalla. Energy-efficient and secure s-box circuit using symmetric pass gate adiabatic logic. In *VLSI (ISVLSI), 2016 IEEE Computer Society Annual Symposium on*, pages 308–313. IEEE, 2016.

[11] Himanshu Thapliyal, Azhar Mohammad, S Dinesh Kumar, and Fazel Sharifi. Energy-efficient magnetic 4-2 compressor. *Microelectronics Journal*, 67:1–9, 2017.

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

[13] Mariana Safta, Paul Svasta, Mihai Dima, Andrei Marghescu, and Mihai-Narcis Costiuc. Design and setup of power analysis attacks. In *Design and Technology in Electronic Packaging (SIITME), 2016 IEEE 22nd International Symposium for*, pages 110–113. IEEE, 2016.

[14] Manfred Aigner and Elisabeth Oswald. Power analysis tutorial, 2000.

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

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

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

[18] Weisheng Zhao, Eric Belhaire, Claude Chappert, and Pascale Mazoyer. Spin transfer torque (stt)-mram–based runtime reconfiguration fpga circuit. *ACM Transactions on Embedded Computing Systems (TECS)*, 9(2):14, 2009.

[19] Paul L McEuen, Michael S Fuhrer, and Hongkun Park. Single-walled carbon nanotube electronics. *IEEE transactions on nanotechnology*, 99(1):78–85, 2002.

[20] Fazel Sharifi, Atiyeh Panahi, Mohammad Hossein Moaiyeri, and Keivan Navi. High performance cnfet-based ternary full adders. *arXiv preprint arXiv:1701.00307*, 2017.

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

[22] Carlos Monteiro, Yasuhiro Takahashi, and Taku Sekine. Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks. In *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*, pages 732–736. IEEE, 2013.

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

[24] Yong Moon and Deog-Kyoon Jeong. An efficient charge recovery logic circuit. *Solid-State Circuits, IEEE Journal of*, 31(4):514–522, 1996.

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

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

[27] Elisabeth Oswald, Stefan Mangard, Norbert Pramstaller, and Vincent Rijmen. A side-channel analysis resistant description of the aes s-box. In *Fast Software Encryption*, pages 413–423. Springer, 2005.

[28] Pete Chown. Advanced encryption standard (aes) ciphersuites for transport layer security (tls). Technical report, 2002.

[29] Daniel V Bailey and Christof Paar. Optimal extension fields for fast arithmetic in public-key algorithms. In *Advances in Cryptology—CRYPTO'98*, pages 472–485. Springer, 1998.

[30] Toshiya Itoh and Shigeo Tsujii. Structure of parallel multipliers for a class of fields gf (2 m). *Information and computation*, 83(1):21–40, 1989.

[31] Chiou-Yng Lee, Erl-Huei Lu, and Jau-Yien Lee. Bit-parallel systolic multipliers for gf (2 m) fields defined by all-one and equally spaced polynomials. *Computers, IEEE Transactions on*, 50(5):385–393, 2001.

[32] Sylvain Guilley, Philippe Hoogvorst, and Renaud Pacalet. Differential power analysis model and some results. In *Smart Card Research and Advanced Applications Vi*, pages 127–142. Springer, 2004.

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

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

[35] William H Kautz. Cellular logic-in-memory arrays. *IEEE Transactions on Computers*, 100(8):719–727, 1969.

[36] Shoun Matsunaga, Jun Hayakawa, Shoji Ikeda, Katsuya Miura, Haruhiro Hasegawa, Tetsuo Endoh, Hideo Ohno, and Takahiro Hanyu. Fabrication of a nonvolatile full adder based on logic-in-memory architecture using magnetic tunnel junctions. *Applied Physics Express*, 1(9):091301, 2008.

[37] Takahiro Hanyu. Challenge of mtj/mos-hybrid logic-in-memory architecture for nonvolatile vlsi processor. In *Circuits and Systems (ISCAS), 2013 IEEE International Symposium on*, pages 117–120. IEEE, 2013.

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

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

[40] Wang Kang, Yi Ran, Weifeng Lv, Youguang Zhang, and Weisheng Zhao. High-speed, low-power, magnetic non-volatile flip-flop with voltage-controlled, magnetic anisotropy assistance. *IEEE Magnetics Letters*, 7:1–5, 2016.

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

[42] Guillaume Prenat, Mourad El Baraji, Wei Guo, Ricardo Sousa, Virgile Javerliac, Jean-Pierre Nozieres, Weisheng Zhao, and Eric Belhaire. Cmos/magnetic hybrid architectures. In *Electronics, Circuits and Systems, 2007. ICECS 2007. 14th IEEE International Conference on*, pages 190–193. IEEE, 2007.

[43] Hao Meng, Jianguo Wang, and Jian-Ping Wang. A spintronics full adder for magnetic cpu. *IEEE Electron Device Letters*, 26(6):360–362, 2005.

[44] Noboru Sakimura, Tadahiko Sugibayashi, Ryusuke Nebashi, and Naoki Kasai. Nonvolatile magnetic flip-flop for standby-power-free socs. *IEEE Journal of Solid-State Circuits*, 44(8):2244–2250, 2009.

[45] Chip-Hong Chang, Jiangmin Gu, and Mingyan Zhang. Ultra low-voltage low-power cmos 4-2 and 5-2 compressors for fast arithmetic circuits. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 51(10):1985–1997, 2004.

[46] Majid Amini Valashani and Sattar Mirzakuchaki. A novel fast, low-power and high-performance xor-xnor cell. In *Circuits and Systems (ISCAS), 2016 IEEE International Symposium on*, pages 694–697. IEEE, 2016.

[47] Jie Deng. *Device modeling and circuit performance evaluation for nanoscale devices: silicon technology beyond 45 nm node and carbon nanotube field effect transistors*. PhD thesis, Stanford University, 2007.

Vita

Azhar Mohammad

Education

JNTU Hyderabad
Bachelor of Technology in Electronics and Communication Engineering, May 2014

Experience

Physical design engineer
October 2018-Present
Renesas Electronics America
Milpitas, CA

R&D intern
May 2018-September 2018
Synopsys
Mountain View, CA

Co-op Masters
September 2017-May 2018
Cypress Semiconductors
Lexington, KY

Publications

Himanshu Thapliyal, Azhar Mohammad, S. Dinesh Kumar and Fazel Sharifi. "Energy Efficient Magnetic 4-2 Compressor." Microelectronics Journal 67 (2017): 1-9.
S. Dinesh Kumar, Himanshu Thapliyal, Azhar Mohammad, Kalyan S. Perumalla. "Design exploration of a Symmetric Pass Gate Adiabatic Logic for energy-efficient and secure hardware." Integration, the VLSI Journal 58 (2017): 369-377.
S. Dinesh Kumar, Himanshu Thapliyal, Azhar Mohammad, Vijay Singh and Kalyan S. Perumalla. "Energy-Efficient and Secure S-Box Circuit using Symmetric Pass Gate Adiabatic Logic." IEEE Computer Society Annual Symposium on VLSI (ISVLSI)(2016): 308-313.
S. Dinesh Kumar, Himanshu Thapliyal, Azhar Mohammad. "EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card." IEEE Transactions on Emerging Topics in Computing (2016).