NORMALLY-OFF COMPUTING DESIGN METHODOLOGY USING SPINTRONICS: FROM DEVICES TO ARCHITECTURES

by

ARMAN ROOHI
B.Sc. Shiraz University, 2008
M.S. Science and Research Branch, Azad University, 2011

A dissertation submitted in partial fulfilment of the requirements
for the degree of Doctor of Philosophy
in the Department of Electrical and Computer Engineering
in the College of Engineering and Computer Science
at the University of Central Florida
Orlando, Florida

Spring Term
2019

Major Professor: Ronald F DeMara

ABSTRACT

Energy-harvesting-powered computing offers intriguing and vast opportunities to dramatically transform the landscape of Internet of Things (IoT) devices and wireless sensor networks by utilizing ambient sources of light, thermal, kinetic, and electromagnetic energy to achieve battery-free computing. In order to operate within the restricted energy capacity and intermittency profile of battery-free operation, it is proposed to innovate *Elastic Intermittent Computation* (EIC) as a new duty-cycle-variable computing approach leveraging the non-volatility inherent in post-CMOS switching devices. The foundations of EIC will be advanced from the ground up by extending Spin Hall Effect Magnetic Tunnel Junction (SHE-MTJ) device models to realize SHE-MTJ-based Majority Gate (MG) and Polymorphic Gate (PG) logic approaches and libraries, that leverage intrinsic-non-volatility to realize middleware-coherent, intermittent computation without checkpointing, micro-tasking, or software bloat and energy overheads vital to IoT.

Device-level EIC research concentrates on encapsulating SHE-MTJ behavior with a compact model to leverage the non-volatility of the device for intrinsic provision of intermittent computation, and lifetime energy reduction. Based on this model, the circuit-level EIC contributions will entail the design, simulation, and analysis of PG-based spintronic logic which is adaptable at the gate-level to support variable duty cycle execution that is robust to brief and extended supply outages or unscheduled dropouts, and development of spin-based research synthesis and optimization routines compatible with existing commercial toolchains. These tools will be employed to design a hybrid post-CMOS processing unit utilizing pipelining and power-gating through state-holding properties within the datapath itself, thus eliminating checkpointing and data transfer operations.

“Dedicated to my beloved parents, my lovely wife, and my older brothers,”

for their love, endless support, encouragement & sacrifices.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to Dr. DeMara who provided an opportunity for me to join the Computer Architecture Laboratory (CAL) research team, and conduct my research under his supervision. He has kindly supported me during this project, and his insightful comments helped me to proceed my research along the right direction leading to several publications in prestigious journals. I would also like to thank my committee members Dr. Enrique del Barco, Dr. Reza Abdolvand, Dr. Jun Wang, and Dr. Deliang Fan for supporting me and my research.

TABLE OF CONTENTS

LIST OF FIGURES x

LIST OF TABLES xvi

CHAPTER 1: INTRODUCTION AND MOTIVATION 1

Introduction 1

Motivation 2

Contributions 4

CHAPTER 2: BACKGROUND 7

Spintronic Concepts, Behaviors, and Switching Operations 7

Magnetic Tunnel Junction (MTJ) 10

MTJ Switching Approaches 12

Field-induced magnetic switching (FIMS) 12

Thermal-assisted switching (TAS) 13

Spin-transfer Torque (SST) 14

Non-volatile spin-based logic 18

Intermittent Approaches 19

CHAPTER 3: COMPACT MODEL OF STT/SHE
FOR BOTH IMTJ AND PMTJ 22

Compact Model Of STT-MTJ 22

MTJ Resistive Model 22

Spin-Transfer Torque (STT) Switching Model 25

STT-MTJ Based Look-Up Table 28

Compact Model Of SHE-MTJ 32

SHE-MTJ Based Look-Up Table 37

CHAPTER 4: SPINTRONICS MAJORITY GATE BASED DESIGNS 40

MG-based Synthesis and Optimization Research Tool 40

Spintronics MG-based Circuit Designs 43

MG-based Full Adder using Current-Induced Domain Wall Nanomagnets 45

MG-based Full Adder using Spin Hall Effect Switching 58

CHAPTER 5: SPIN-BASED NORMALLY-OFF COMPUTING APPROACHES 68

NV FFs For Normally-Off Computing 69

NV-Assisted Power Gating 70

NV-Enabled Intermittent Computing 71

SHE-based Majority Gate Cell Library 73

Proposed SORT Approach and SHE Technology Library Generation 75

Technology-Dependent Optimization 77

Power and Delay Optimization 79

Area Optimization 82

Simulation Results 82

NV-Clustering Design Methodology 87

Logic-Embedded FF (LE-FF) Design 88

NV-Clustering Methodology 91

Simulation Results 96

Area Analysis 98

Power Analysis 101

Delay Analysis 103

Resumption Overhead 104

CHAPTER 6: SECURE INTERMITTENT-ROBUST POLYMORPHIC GATE-BASED DESIGN 108

Secure Intermittent-Robust Computation for IoT Devices 108

Vulnerabilities under Charging Attacks 109

111section*.51

Logic-Encrypted Synthesis for Spintronic-Embedded Datapath Design 116

116section*.53

Secure PG-FF design 117

PG insertion methodology 119

Simulation Results 121

Area Analysis 122

Power-Delay Analysis 124

CHAPTER 7: CONCLUSION AND FUTURE WORK 127

Technical Summary 127

Future Work 131

APPENDIX A: COPYRIGHT PERMISSIONS 132

LIST OF REFERENCES 140

LIST OF FIGURES

Figure 1.1: Five required STEPs in the thesis to implement a new intermittent computing method for IoT applications. 6

Figure 2.1: Energy barrier of a spin-based device. 8

Figure 2.2: GMR effect, (a) parallel state, and (b) anti-parallel state. 9

Figure 2.3: Parallel and anti-parallel configurations of a TMR device. 10

Figure 2.4: (a) MTJ vertical structure [1], (b) In-plane MTJ (IMTJ), and (c) Perpendicular MTJ (PMTJ). 12

Figure 2.5: FIMS approach for MTJ. 13

Figure 2.6: TAS approach for MTJ. 14

Figure 2.7: Spin-transfer torque concept, (a) if electrons flow from the PL to FL, the magnet is switched to P state, and (b) if electrons flow from the FL to PL, the magnet is switched to AP state. 15

Figure 2.8: Magnetization dynamics for a magnet in the presence of STT. 16

Figure 2.9: (a) Positive current along +x induces a spin injection current +z direction. The injected spin current produces the required spin torque for aligning the magnetic direction of the FM in +y directions, (b) Top view. 18

Figure 2.10Main magnetic logic architectures, (a) MQCA [2], (b) DWL [3], (c) ASL [4], and (d) MTJ-based logic cell [5, 6]. 19

Figure 3.1: Resistance hysteresis of an MTJ, red arrow shows switching from AP to P, while blue arrow indicates switching from P to AP. 24

Figure 3.2: Illustrations (a) in-plane and (b) out-of-plane or perpendicular magnetized MTJ. 27

Figure 3.3: Four-input STT-LUT functional diagram. 29

Figure 3.4: Reference MTJ cell and LUT MTJ cell dimensions. 30

Figure 3.5: Transient response of STT-LUT for four-input NAND operation for (top) ABCD = "1111" and (middle) ABCD = "0000". 32

Figure 3.6: SHE-MTJ vertical structure. Positive current along +x induces a spin injection current +z direction. The injected spin current produces the required spin torque for aligning the magnetic direction of the free layer in +y directions, and vice versa. (b) SHE-MTJ Top view. 33

Figure 3.7: (a) 2-terminal MTJ (STT-MTJ) bit-cell, (b) 3-terminal (SHE-MTJ) bit-cell. . 36

Figure 3.8: Circuit-level design of proposed SHE-LUT. 37

Figure 4.1: Two chromosomes (a) before crossover, and (b) after crossover. 44

Figure 4.2: Schematic of a 1-bit full adder using 3- and 5- input MGs. 45

Figure 4.3: STT-driven Domain Wall motion. 46

Figure 4.4: (a) Schematic illustration of DWNM device, (b) construction of a DWNM logic gate suitable for Boolean logic implementation. 47

Figure 4.5: DWNM (a) cell design, and (b) cross sectional view. 48

Figure 4.6: Schematic of DWNM based Full-Adder Circuit. The main structure is comprised of two DWNMs and two SAs, which operate as the functional building blocks and the decision-making elements, respectively. 49

Figure 4.7: Simulation results of 1-bit DWNM based FA. Logic 0/1 levels of inputs (A, B, and C) correspond to applied currents of -200A and +200A whereas bits 0 and 1 for outputs, Cout and SUM, correspond to the voltage of 0V and 1.8V. For instance, input current pulses ABC=011 nucleate the DW in nanowire-1, Cout=1, and cannot unpin the DW in nanowire-2, SUM=0. 51

Figure 4.8: Dependence of DWNM-FA Average Delay on Input Current are depicted for circuit outputs Cout and SUM. 54

Figure 4.9: Power Consumption of DWNM-FA versus temperature and applied current. . 56

Figure 4.10 PDP of DWNM-FA versus temperature and applied current. 57

Figure 4.11 Circuit-view of SHE-based FA design. SHE-1 functions as a 3-input MG, while SHE-2 performs 5-input MG function. 58

Figure 4.12 SHE-based functionality for input ABC = "010" (a) write and reset operations for SHE-1 and SHE-2 occurred, respectively, I_{input} = 94 μA $< I_{C\text{-}SHE1}$; hence, FL of SHE-1 remains in P state, then (b) read and write operation for SHE-1 and SHE-2 perform simultaneously, in which injected current through SHE-2 is 146 μA $> I_{C\text{-}SHE2}$, so FL of SHE-2 changes to AP state, and finally (c) SHE-1 is reset along with reading SHE-2 state. 63

Figure 4.13Simulation results of 1-bit SHE-based FA for two input sequences, “010” and “111”. 64

Figure 4.14Schematic of 4-bit SHE-based FA and its timing diagram. 66

Figure 5.1: Block diagram of NV-FFs, (left) modified slave stage, and (right) modified master stage. 71

Figure 5.2: Overall structure of intermittent resilient architecture. 72

Figure 5.3: (a) SHE-MTJ based 3-input MG, (b) SHE-MTJ based 5-input MG. Simulation results for (c) 2-input OR logic, and 3-input AND logic using MG3 and MG5, respectively, (d) 3-input and 5-input SHE-MTJ based MGs. 74

Figure 5.4: Proposed MG synthesis approach to realize SHE-based Boolean Logic, including SHE-MG based gate libraries. 75

Figure 5.5: Schematic of the proposed evolutionary approach to realize MG- based NoC circuit. 76

Figure 5.6: Operations of F1 and F2 blocks for AB+C in technology-dependent optimization process. 79

Figure 5.7: (a) technology-dependent optimization for F= A.B.C.D, (b) power optimization for F= A+B+C+D, (c) area optimization for F= A(B+CD), and (d) comparison results for Designs in (b) and (c). 84

Figure 5.8: Normalized results for (a) power consumption, and (b) delay leveraging two optimization approaches. 85

Figure 5.9: Optimized NV implementation methodology diagram. 87

Figure 5.10: (a) Schematic of proposed MG-based LE-FF, and (b) different implementations using NV-FF (top), and proposed LE-FF (bottom). 90

Figure 5.11: All three sensitive time durations for (a) NV-FF based implementation, and for (b) proposed implementation approach, in which C1(b) $<$ C1(a). 90

Figure 5.12: (a) s27 schematic with highlighted FFs, and (b) optimized LE-FF based design after NV-Clustering. 95

Figure 5.13: Circuit-level design of proposed 3-input SHE-based LE-FF, and (b) transient response for three different input ABC= “001”, “111”, and “000” in presence of power failure. Three different modes are shown: (1) store mode, (2) standby mode, and (3) sense mode. 98

Figure 5.14: Normalized area consumption compared to CMOS-based implementations for different benchmarks. 100

Figure 5.15: Normalized power dissipation compared to NV-FF. Results based on realization of combinational components. 102

Figure 5.16: Total power consumption for selected ISCAS-89 circuits. 102

Figure 5.17: Normalized delay compared to NV-FF based implementations for different benchmarks. 103

Figure 5.18: Normalized PDP compared to NV-FF based implementations for *intermittency-absent* and *intermittency-present* scenarios. 107

Figure 6.1: (a) SIRC computation pool of NV-MGs, (b) NV-FA arrangement using 3-MG and 5-MG, and (c) 2-bit NVM multiplier. 109

Figure 6.2: Feasible countermeasure for charging attack by marking a possible malicious node. 111

Figure 6.3: Power masking countermeasure for possible power analysis attack. F1 and F2 perform the same function with different power consumption. 113

Figure 6.4: `s27` schematic (top left), selected cone gate (bottom left), developed MG-FF based design (top right), and equivalent logic realizations (bottom right). . . . 115

Figure 6.5: Power traces results for all possible K_1K_2 combinations. 116

Figure 6.6: (a) SH-MTJ based 3-input PG, (b) 2-input OR, NOR, AND and NAND logic using 3-input PG, (c) 3-input and 5- input SHE-MTJ based PGs, (d) 5-input PG Functional Modes. 118

Figure 6.7: Normalized area consumption compared to CMOS-based implementations for ISCAS, ITC, and MCNC benchmarks. 125

Figure 6.8: Normalized PDP compared to NV-FF based implementations for ISCAS, ITC, and MCNC benchmarks. 126

LIST OF TABLES

Table 2.1: Characteristics of enabling technologies. "✓" or "-" indicates strength/limitation relative to CMOS. 20

Table 2.2: Selected previous works with significant contributions towards intermittent processor design. 21

Table 3.1: performance comparison between STT-LUT and SRAM-LUT for four-input NAND operation. 30

Table 3.2: Performance comparison for four-input NAND operation. 31

Table 3.3: Parameters of SHE-MTJ-based LUT. 35

Table 3.4: Switching Characteristics of a Single MTJ Cell Including Clocking Requirements. 36

Table 3.5: Performance comparison for the Reconfiguration Operation of 4-input MTJ-LUTs Involving 16 MTJs. 39

Table 4.1: Optimization of three standard functions. 43

Table 4.2: Simulation Parameters of DWNM and MTJs. 52

Table 4.3: Nanowire-1(for Cout) and Nanowire-2 (for SUM) Switching Delays. 53

Table 4.4: Comparison of 1-bit Full Adders. 57

Table 4.5: Simulation Parameters of SHE-based FA. 60

Table 4.6: Required signaling for 1-bit SHE-based FA. 61

Table 4.7: SHE-based FA Performances for all Input Combinations. 64

Table 4.8: Comparison of logic-in-memory 1-bit full adder circuits. 65

Table 5.1: Switching results for 3-input SHE-MG. 73

Table 5.2: Switching results for 5-input SHE-MG. 74

Table 5.3: Read operation results for 3- and 5- input SHE-MGs. 74

Table 5.4: Optimized implementation of the functionally-complete set of Boolean logic gates using SHE-MGs. 86

Table 5.5: Boolean Expressions using 3 and 5 -input MGs. 90

Table 5.6: Gate Counts for s27 Benchmark Circuit. 97

Table 5.7: NV-Clustering Gate Equivalent Reduction. 99

Table 6.1: Generated Keys and Their Corresponding Average Power Consumption. . . . 115

Table 6.2: PG-insertion results for ISCAS benchmarks. 123

CHAPTER 1: INTRODUCTION AND MOTIVATION

Introduction

For the past five decades, complementary metal-oxide-semiconductor (CMOS) has been the dominant technology and it has provided the demanded dimension scaling for implementing high-performance and low-power circuits. The evolution of this charge-based CMOS devices is described and predicted by Moore's law [7], this prediction, that number of transistors in integrated circuits (ICs) doubles roughly every two years, has continued for many years. On the other hand, by the inevitable scaling down of the feature size of the CMOS transistors which are deeper in nanoranges, the CMOS technology has encountered many critical challenges such as high leakage currents, reduced gate control, high power density, increased circuit noise sensitivity and high lithography costs which obstruct the continuous dimension scaling and consequently degrade the suitability of the CMOS technology for the near future high-density and energy efficient applications. Explaining in more details about the first aforementioned restriction, due to the quantum mechanical tunneling of electrons from the gate electrode into the transistor channel through the gate oxide, leakage current occurs. Owing to the Moor's law's and mentioned problems as well as the increasing chip complexity, researchers have to start seeking novel technologies to replace the charge-based devices. Among promising devices, 2015 International Technology Roadmap for Semiconductors (ITRS) [8] identifies nanoscale devices as capable post-CMOS candidates such as Quantum-Dot Cellular Automata (QCA) [9, 10], and Spintronics [11, 12] (feasible competitive alternative). Spintronics devices show promising features such as non-volatility, near-zero static power, and high integration density. The non-volatility means that the data can be maintained even if the power is off, so the standby power is reduced significantly. Moreover, due to the possibility of 3D integration above CMOS designs at the back-end process, distances between logic and

memory can be shortened, which reduces considerably the dynamic power. The scalability feature of spin-based devices in addition to their low power characteristic, make the Spintronics as a promising alternative for CMOS architectures.

Recently, magnetic tunnel junction (MTJ) devices are one of the most important components of any spin-based structures, which can be configured into two different stable configurations. Due to the tunnel magnetoresistance (TMR) effect, these two parallel and anti-parallel states show low and high resistance, which can be denoted "0" and "1" in binary information, respectively. Two of developed switching approaches for MTJs are spin-transfer torque (STT) [13] and spin-Hall effect (SHE) [1], in which only one bidirectional current is required. In the STT switching approach, the bidirectional current passes through an MTJ according to which it can be configured into P or AP state. Although STT offers several advantages over previous switching methods like field-induced magnetic switching (FIMS) [14] and thermally assisted switching (TAS) [15], it suffers from some challenges such as high write current, and switching asymmetry [16, 17]. Moreover, STT-MTJ is a two-terminal device with a shared write and read path. Consequently, undesirable switching may occur during the read operation, and stored data can be flipped accidentally. Recently, SHE-MTJ, a 3-terminal device, has been researched as a potential alternative offering some benefits such as decoupled read and write paths, as well as energy efficient and high-speed write [18, 19, 20].

Motivation

Intermittent computation approach offers intriguing and vast opportunities to dramatically transform the landscape of IoT devices. The Internet of Things (IoT) devices require drastically-reduced energy consumption such that they are able to operate using only ambient sources of light [21, 22], thermal [21, 23], kinetic [21, 24], and electromagnetic energy [25] as a means to achieve battery-free computing [26]. If lightweight embedded computing could be realized with free and/or inex-

haustible sources of energy, new classes of maintenance-free, compact, and inexpensive computing applications would become possible [27]. Thus, energy-harvesting-powered devices could enable a sustainable computing platform for future medical [28], aerospace [29], and IoT [30] applications. Energy-harvesting devices are projected to develop towards a $2.6B market by 2024, thus automating human interaction with everyday items in our environment or even life-saving medical implants within our bodies [31].

Therefore, it is proposed to research a promising class of rudimentary processing elements which utilize switching devices capable of leveraging (1) the restricted energy capacity and (2) the intermittent temporal energy profile, of energy harvesting schemes. A typical energy harvesting system converts ambient energy via rectification and charge-trapping. Then energy is accumulated on capacitor to generate a supply voltage. Once the voltage of the capacitor attains a sufficient level, then a lightweight embedded processing element can commence its operation. However, the stored energy will be rapidly consumed, which consequently precludes the continuation of execution due to an insufficient supply voltage. Hence, the supply voltage of the processor experiences intermittent behavior. This results in an interval, τ_{idle}, of unpredictable unavailability that can interrupt the datapath and the processor clock. This charge/discharge cycle, which is an intrinsic characteristic of energy harvesting devices, may occur more than hundreds of times per second for RF-based sources, and unpredictably for extended durations with kinetic and light-powered sources. Furthermore, the interval τ_{idle} can occur irregularly and vary in duration leading us to research methods to achieve a new Elastic Model of Computation described herein. Hardware realization of elastic computing addresses one of the major hurdles to the propagation of energy harvesting systems: robust operation despite discontinuities in the ambient energy supplied from its environment. Robust intermittent operation presents a new and difficult technical challenge that precludes assumptions of conventional processor design of the last several decades. Intermittent behavior can result in disturbances in the execution of programs, data loss, glitch conditions, and lack of execution progress

that may lead to irregular and unpredictable results [32]. Therefore, most of the existing energy harvesting systems are envisioned for rudimentary signal detection and sensing applications such as monitoring blood pressure or accumulating temperature readings [33]. This proposed herein could realize these at improved lifetime energy and area metrics.

***Grand Hypothesis*: The proposed circuits employing spintronic devices realize Elastic Intermittent Computation enabling a non-deterministic duty cycle, while reducing leakage energy by 90% and circuit lifetime energy-delay-product by 60% compared to existing designs of comparable area.**

Regardless if the hypothesis is validated or not, the proposed research will advance multiple promising directions towards beyond-CMOS devices and architectures for next energy harvesting powered processors.

Contributions

Due to the abovementioned research background and motivation, four objectives are addressed: First, to explore the energy and delay characteristics of spin-based VLSI circuits as well as innovate novel architectural schemes utilizing non-volatile logic, by integrating Verilog-A and SPICE models, a compact model for STT-IMTJ, STT-PMTJ, and SHE-IMTJ are developed. They express the underlying both static and dynamic switching behavior and encapsulate their characteristics, while allowing straightforward integration with VLSI circuits in SPICE-like platforms. To validate the model, two STT and SHE Look-up Table (LUT) circuits are designed and their functionalities are verified.

Second, a Genetic Algorithm (GA)-driven research synthesis and optimization MG-based is developed. Extracting the fan-in optimized design based on 3- and 5- input MGs to design Boolean logic

gates and logic circuits such as Full-Adders (FAs). Two novel designs of the 1-bit majority gate (MG) based full adder (FA) using domain wall nanomagnet (DWN) and SHE-MTJ are proposed. These emerging designs achieve significant improvements in terms of area, complexity and power consumptions. Then SHE-based 3- and 5- input MGs library developed.

Third, Then, preliminary results of the modeled SHE-MTJ devices will be utilized to delineate the power, delay, and area costs of the spin-based building blocks in the synthesis and optimization tool. The Boolean functions and criteria can be applied as inputs into the tool, which outputs a SPICE syntax compatible file that can be utilized by circuit simulation toolchain.

Forth, the developed tool is used to extract an optimized netlist for standard majority logic-based gates such as AND, OR, NAND. New libraries containing a functionally-complete set of Boolean logic gates required for implementing representative VLSI designs will be defined and populated using the developed device models. To verify the functionality and demonstrate energy and performance characteristics, we will implement MCNC benchmark circuits in commercial synthesis tools utilizing the developed spin-based gate libraries.

Finally, circuit-level results will be extended towards benchmark studies corresponding to lifetime energy reduction and intermittent operational behavior demanded by IoT applications. Both goals can be achieved by utilizing the non-volatility of the targeted devices to enable gate-level pipelining, without requiring registers for each stage. Thus, an intermittent operation is supported without the burden of additional circuitry otherwise required for checkpoint-restore, backup, etc. Avoiding registers also provides significant area reduction, which is important to achieve IoT size/cost constraints.

The steps of the work in this document can be depicted in Figure 1.1 from the device to the architecture hierarchy.

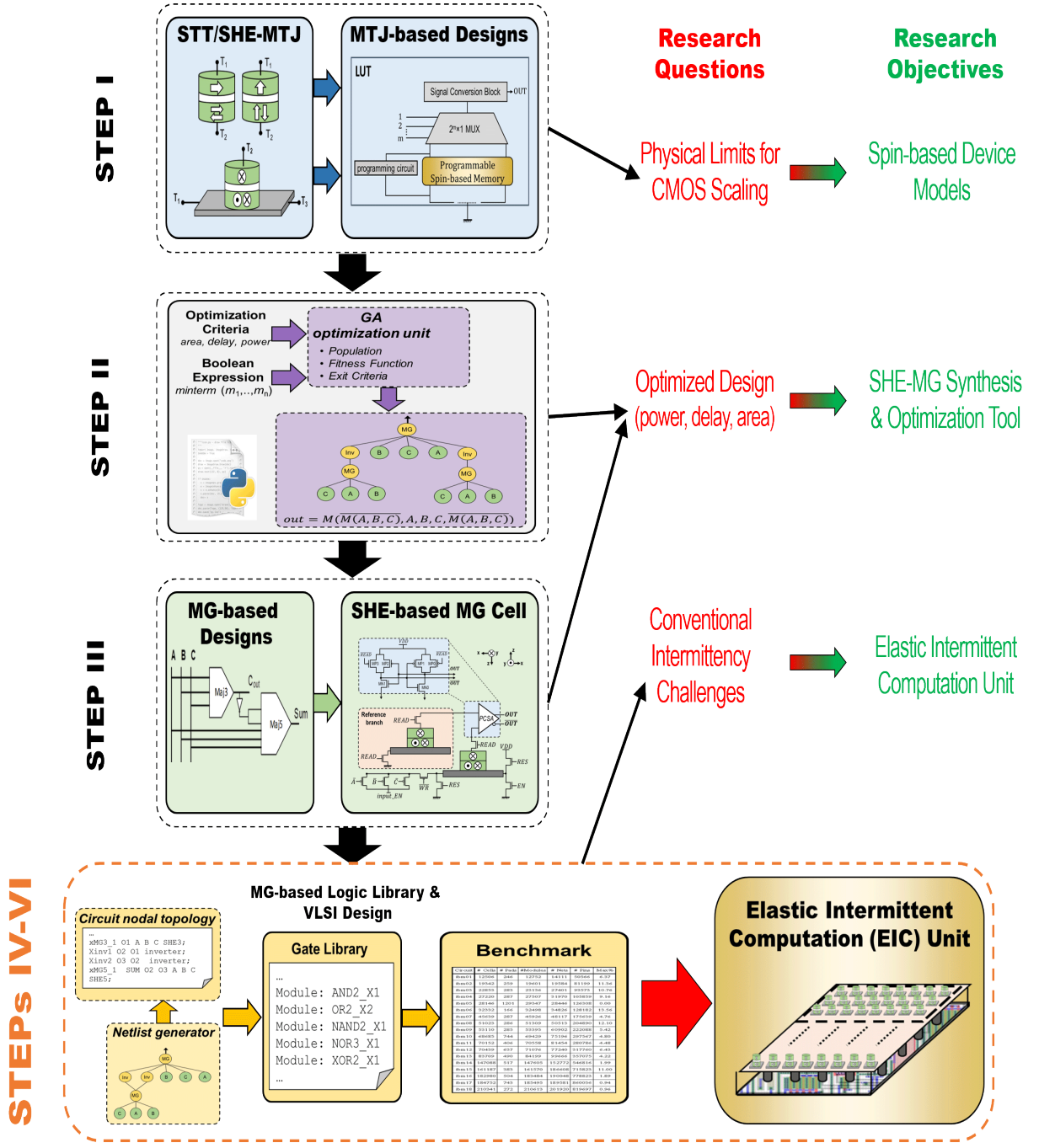


Figure 1.1: Five required STEPs in the thesis to implement a new intermittent computing method for IoT applications.

CHAPTER 2: BACKGROUND

Spintronic Concepts, Behaviors, and Switching Operations

Spin transport electronics (Spintronics) is a novel computing paradigm, which functions regarding the degree of electron spin in solid-state electronics using spin-polarized current [34]. Since spin-based devices are built on magnets, they have two stable polarizations, 0° and 180° magnet spin momentum, which denote up-spin and down-spin, respectively. These two states can be maintained in a magnet without any electrical power, non-volatility, due to its energy barrier (E_B). The relation between the information retention time and the energy barrier is expressed by Equation 2.1:

$$T_{retention} = T_0 \, e^{(\frac{E_B}{K_B T})}, \quad E_B = K_u V \tag{2.1}$$

where T_0 is the characteristic time K_B is the Boltzmann's constant, T is the temperature, K_u is the magnetic anisotropy, and V is the magnet volume. In most spin-based memory and logic implementations, E_B set to 40 which results in ten years for $T_{retention}$. The two stable states regarding E_B are shown in Figure 2.1.

Concept of Spintronics can be defined by two main aspects: (1) spin polarization and (2) magnetoresistance, which are utilized to perform write and read operations, respectively. The imbalance of up-pin ($n \uparrow$) and down-spin ($n \downarrow$) population in ferromagnetic (FM) devices can be considered as spin population, which is defined as

$$P = \frac{|n \uparrow - n \downarrow|}{n \uparrow + n \downarrow} \tag{2.2}$$

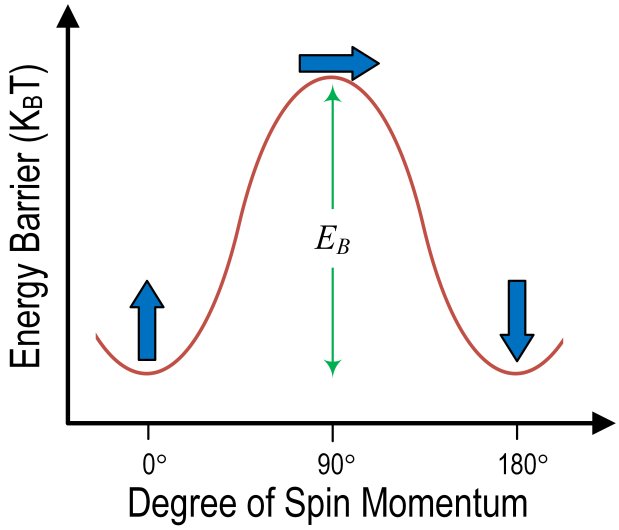


Figure 2.1: Energy barrier of a spin-based device.

When a charge current passing through an FM, it can be polarized according to the local magnetic momentum, hence, a spin-polarized current can be produced. The magnetoresistance is affected by scattering of electrons on the FM layers. There is a high or low magnetoresistance (MR) for magnetic materials, which is used to detect the states of magnetic devices. The two most important MR effects in metal multilayer films are Giant Magnetoresistance (GMR) [35, 36] and Tunneling Magnetoresistance (TMR) [37, 38]. The GMR devices are composed of two FM layers which are separated by a nonmagnetic metal layer such as copper. If magnetization directions of two FM layers are same, parallel (P) configuration, one of the spin-up or spin-down electrons pass through the device without scattering, which leads to lower resistance. Whereas, if magnetization directions of these FM layers are in the anti-parallel configuration (AP), both spin-up and spin-down electrons face scattering issue, which results in higher resistance. Due to the difference between the P and AP configurations, which can reach 100%, this MR effect named giant magnetoresistance. The highly-used GMR-based application is a spin valve concept, which has been leveraged in conventional hard disk drives as reading heads. Figure 2.2 depicts the GMR effect in two-channel multilayer

films. If we replace the non-magnetic layer in a GMR structure by a thin oxide insulator such as AlxOy [39] and MgO [40], TMR effect can be detected.

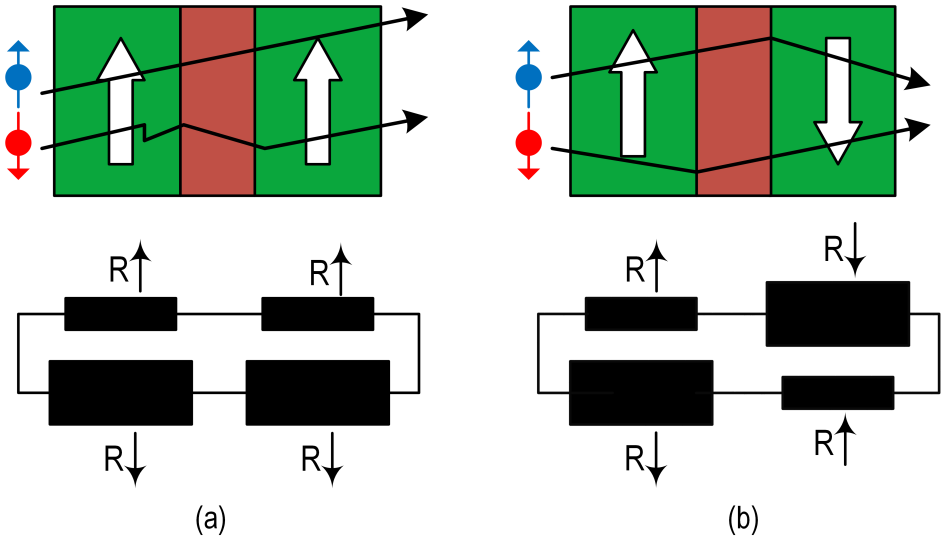


Figure 2.2: GMR effect, (a) parallel state, and (b) anti-parallel state.

This spacer is enough thin to allow tunneling effect for the electrons. Figure 2.3 shows a TMR device and its two stable states. Similar to the GMR effect, TMR can define P and AP magnetization orientations by two different low and high resistances, respectively. However, in addition to the difference in barrier material for GMR and TMR devices, there are two main differences.

First, in GMR structure, current flows in both “in the layer plane” (CIP) or “perpendicular to plane” (CPP) [41], however, in TMR, current can pass only in a perpendicular way. Second, in GMR, all its layers are a conductor, which means the larger current is transferred, nonetheless, in TMR devices, we have an insulator, which is preferable in non-volatile memory and logic designs.

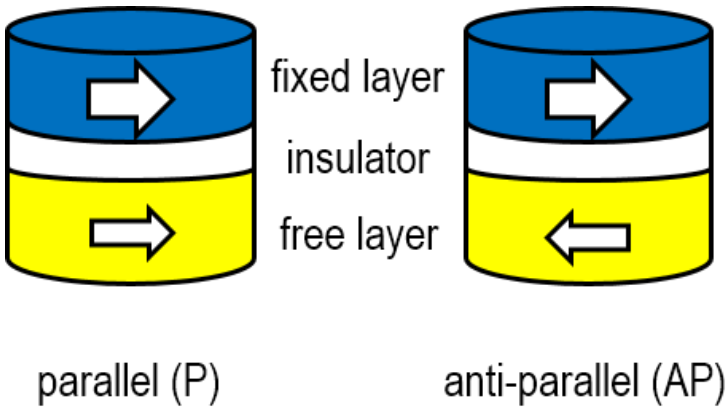


Figure 2.3: Parallel and anti-parallel configurations of a TMR device.

Magnetic Tunnel Junction (MTJ)

The vertical structure of an MTJ is shown in Figure 2.4 (a), where an insulating barrier is sandwiched between two FM layers, Pinned Layer (PL) and Free Layer (FL) [42]. The barrier is enough thin to enable the electron tunneling effect. Each FM layer has a magnetization which can be switched by a magnetic field between two stable directions along the anisotropy axis. Because these layers have different coercivities, which is defined as the magnetic field to switch the magnetization, PL is magnetically-pinned and utilized as a reference layer, while the FL magnetic orientation can be switched to be parallel (P) or anti-parallel (AP) to that of the PL, which gives a low (RP) or high (RAP) tunneling resistance, respectively, as shown in Figure 2.4 (b). This resistance is specially called tunneling magnetoresistance (TMR) and the mechanisms behind the TMR effect is spin-dependent tunneling, which actually was observed and proposed by Jullière as early as 1975 [42]. The primary performance for an MTJ is determined by TMR ratio which can be defined as

$$TMR = \frac{\Delta R}{R_P} = \frac{R_{AP} - R_P}{R_P} = \frac{G_P - G_{AP}}{G_{AP}} \tag{2.3}$$

where G_P and G_{AP} are the conductances of parallel and anti-parallel states. The expressions of conductance are given by

$$\begin{aligned} G_P &= N_{M1}N_{M2} + N_{m1}N_{m2} \\ G_{AP} &= N_{M1}N_{m2} + N_{m1}N_{M2} \end{aligned} \tag{2.4}$$

where N_{M1} and N_{m1} are the effective densities of states of majority and minority electrons at the Fermi energy in both magnetic layers. As a result, the TMR ratio can be calculated using Equations 2.2, 2.3 and 2.4, which is expressed in terms of the spin polarization by

$$TMR = \frac{2P_1P_2}{1 - P_1P_2} = \begin{cases} R_P = \frac{2}{1+P_1P_2} \\ R_{AP} = \frac{2}{1-P_1P_2} \end{cases} \tag{2.5}$$

where P_1 and P_2 are spin-polarizations in two layers. The significant progress was occurred in 1994 by using amorphous Al_2O_3 as the tunneling barrier to realizing the room temperature magnetic tunneling transport [38, 43]. By optimizing the material and fabrication condition, the TMR ratio of this structure can reach up to 70% [39]. Although this value is already much larger than GMR in spin valve, it is still far away from the requirement for spintronic applications, for example, high-density MRAM requires at least 150% TMR at room temperature. Another considerable leap of MTJ is using a single-crystal MgO tunnel barrier that can provide even larger TMR, which is sometime called the giant TMR effect [44, 45]. So far, the TMR ratio record of MgO based MTJ can reach as high as 600% at room temperature [46]. These results are of great importance not only to avoid the CMOS process mismatch and parameter variation, but also to miniaturize the sense amplifier circuit area [47].

The magnetic direction of MTJ layers can be in the film plane, in-plane MTJ (IMA), or out of the film plane referred to as perpendicular MTJ (PMA) structure, as shown in Figure 2.4 (b) and

2.4(c), respectively. PMAs have advantages over IMAs such as lower switching critical current and higher thermal stability.[1].

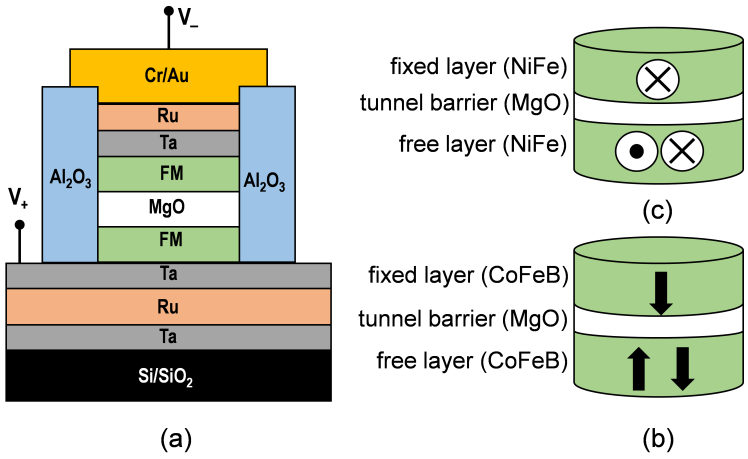


Figure 2.4: (a) MTJ vertical structure [1], (b) In-plane MTJ (IMTJ), and (c) Perpendicular MTJ (PMTJ).

MTJ Switching Approaches

The write operation of an MTJ is achieved by switching the FL magnetization. Herein, brief efficient write methods for MTJ are introduced.

Field-induced magnetic switching (FIMS)

In this approach, the magnetization orientation of the free layer is switched by applying an external magnetic field, which is generated by two orthogonal current lines, the word line (WL) and bit line (BL), as shown in Figure 2.5. To perform a write operation, two currents, I_w and I_b, are applied to

[1]©2016 IEEE. Reprinted, with permission, from [48, 49]

WL and BL, which generate the hard-axis, H_w, and easy-axis, H_b, switching fields, respectively. Herein, H_w equals $2K_u/M_s$ where M_s is the saturation magnetization is applied perpendicular to the easy axis. Then this field is removed and a smaller bias field is applied along the easy axis to complete the switching process. The read operation of this written structure is performed by the current passing through BL. Independent sensing path with writing line is the main advantage of this approach. Nonetheless, in the write operation, a combination of two perpendicular currents results leads to the narrow write margin and half-selectivity issues. Moreover, in order to perform a proper write operation in FIMS, generating magnetic fields is require high currents, $\sim$10 mA, which limits the scalability of FIMS, due to the electromigration effect. To alleviate these issues, there are several solutions were proposed [50], however, the FIMS still suffers from low speed, large area overhead, and high power consumption.

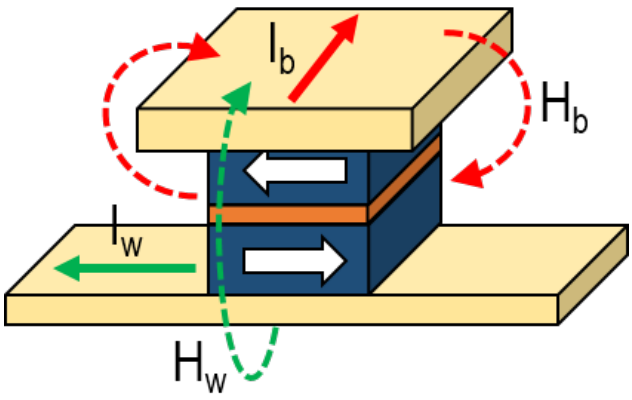


Figure 2.5: FIMS approach for MTJ.

Thermal-assisted switching (TAS)

Thermal-assisted switching (TAS) improves the performance of the FIMS approach in terms of power consumption and thermal stability [15], as shown in Figure 2.6. Its concept is that a current

flowing through MTJ heats the magnetic free layer and reduces greatly the required switching field [51]. Similar to the FIMS structure, two orthogonal current lines are applied to achieve write selectivity; However, one line (I_h) is used to heat the MTJ FL and the other (I_b) is used to generate the switching field. This approach promises relatively lower power, higher density, and higher thermal stability compared with the pioneering FIMS approach. Nevertheless, due to the heating and cooling processes, TAS has a lower operation speed than FIMS.

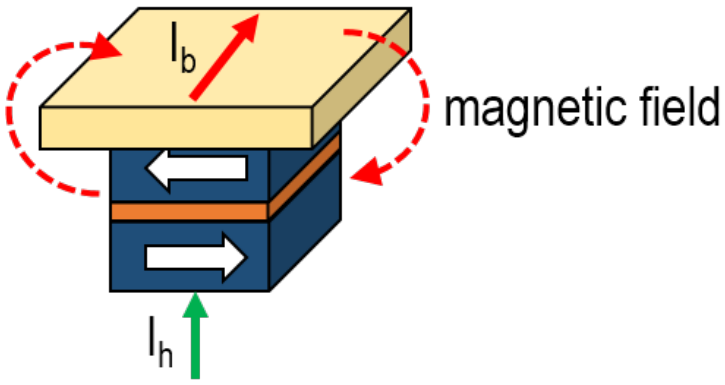


Figure 2.6: TAS approach for MTJ.

Spin-transfer Torque (SST)

In addition to the aforementioned switching approaches, magnets can be switched with spin-torque induced by applying spin-polarized current. This spin-polarized current can be produced using a spin-polarizer (PL) or leveraging spin-Hall effect (SHE) [1, 52]. This non-magnetic field switching idea was fulfilled by Berger and Slonczewski [13] to eliminate the drawbacks of FIMS and TAS. While electrons flow from the PL to FL, they are spin-polarized by the PL and acquire a spin angular momentum nearly aligned to the PL magnetization. After these spin-polarized electrons pass into the FL, their transverse angular momentum must be transferred to the FL magnetization due

to the conservation of angular momentum. Once the amount of electrons exceeding the threshold value, critical current, the spin-transfer torque (STT) exerted by the current will switch the magnetization of the FL to parallel with respect to the PL. If the charge current flows along the opposite direction, they will be spin-polarized against the PL magnetization by the reflection from the RL. In this case, the magnet is switched to AP state by the STT. Figure 2.7 illustrates the principle of STT switching.

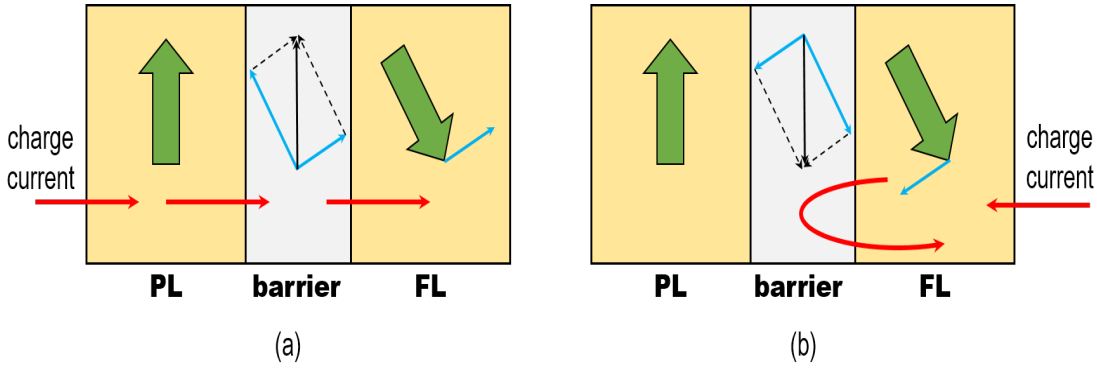


Figure 2.7: Spin-transfer torque concept, (a) if electrons flow from the PL to FL, the magnet is switched to P state, and (b) if electrons flow from the FL to PL, the magnet is switched to AP state.

To understand the STT-induced magnetization switching, the FL magnetization is abstracted to a unit magnetic moment $\vec{m}$ under the macrospin approximation. Then the dynamics of magnetization switching can be described by a Landau-Lifshitz-Gilbert (LLG) equation [53] including the STT, as:

$$\frac{\partial \vec{m}}{\partial t} = -\gamma\mu_0 \vec{m} \times \vec{H}_{eff} + a\left(\vec{m} \times \frac{d\vec{m}}{dt}\right) - \frac{\gamma\hbar JP}{2et_{ox}M_s}\vec{m} \times (\vec{m} \times \vec{m}_r) \tag{2.6}$$

where $\vec{H}_{eff}$ is the effective magnetic field, which is the sum of different magnetic fields, such as the external magnetic field, the demagnetization field and the anisotropy field. γ is the gyromagnetic ratio. μ_0 is the permeability in the free space. a is the Gilbert damping constant. $\hbar$ is the reduced Planck constant, P is the spin-polarization, e is the elementary charge, t_{ox} is the FL thickness,

M_s is the saturation magnetization, $\vec{m}$ is the unit vector along the PL magnetization, J is the write current density. Three torques are introduced in Equation 2.6, which are shown in Figure 2.8 [54, 55]. The first torque is the field-induced torque which causes the magnetic moment to process around the effective magnetic field. The second torque is the Gilbert damping torque which relaxes the precession. The final torque term is the STT, which is proportional to the charge current density and due to the polarity of injected current, it can help or resist the Gilbert damping torque. For instance, if the applied current density is larger than the critical current density, the exerted STT can compensate the Gilbert damping torque and switches the FL magnetization. Due to the simplicity of STT implementation, scalability, lower read energy, and higher read speed than FIMS and TAS, it has become the main switching approach for two-terminal Spintronics devices including GMR [41, 56] and TMR devices [57, 58]. In this approach, the common path is utilized for both write and read operations, which can lead to accidental write operation during reading. Moreover, a significant incubation delay due to the pre-switching oscillation [16, 59] incurs high switching energy. Therefore, recently, SHE is proposed for 3-terminal spin-based TMR devices as an alternative, which provides separate paths for reading and write operations, while expending significantly less switching energy [18, 19, 60].

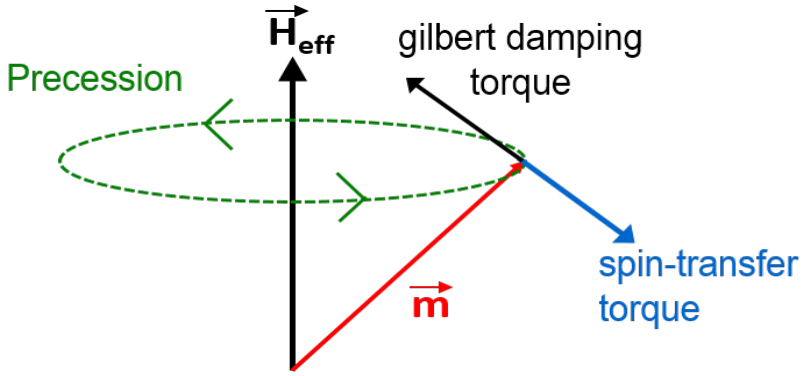


Figure 2.8: Magnetization dynamics for a magnet in the presence of STT.

It is shown in [61] that a spin-polarized current, which is used to generate torque, can be produced in nanomagnetic devices by the spin-Hall effect (SHE) rather than passing charge current through an FM in spin polarizer approach. Figure 2.9 shows the spin-Hall effect phenomenon. The FM layer is directly connected to heavy metal (HM) which is normally made of β-tantalum (β-Ta) [1], β-tungsten (β-W) [62] or Pt [63]. By applying charge current to the left terminal of HM, electrons flow through an HM in $\pm$x direction. The spin-orbit coupling in HM deflects the electrons with different spins in opposite directions, which results in a spin injection current in the $\pm$z direction transverse to the applied charge current. This generated spin-polarized current exerts STT on the above FM and based on the direction of the injected charge current the FM magnetization can be switched to P or AP states, as shown in Figure 2.9. Ratio of the injected spin current to the applied charge current, called spin Hall injection efficiency (SHIE), is defined by Equation 2.7:

$$SHIE = \frac{I_S}{I_C} = \frac{A_{FM}}{A_{HM}} \times \sigma\theta_{SH} \tag{2.7}$$

where A_{FM} and A_{FM} are the cross-sectional areas of the HM, and the adjacent FM area, respectively. θ_{SH} is the spin Hall angle, the ratio of generated spin current density to the applied charge current density, and σ is the electron spin polarization. If the right side of the above equation is larger than 1, then the spin-polarized current is larger than the charge current. Due to the difference in scattering ratio of electrons at the HM and FM interface, the spin-transfer efficiency in FM is lower than HM; Hence, the SHIE is larger than 1, which shows high efficiency for SHE usage. STT and SHE switching approaches for MTJ will be discussed in more details in the next chapters.

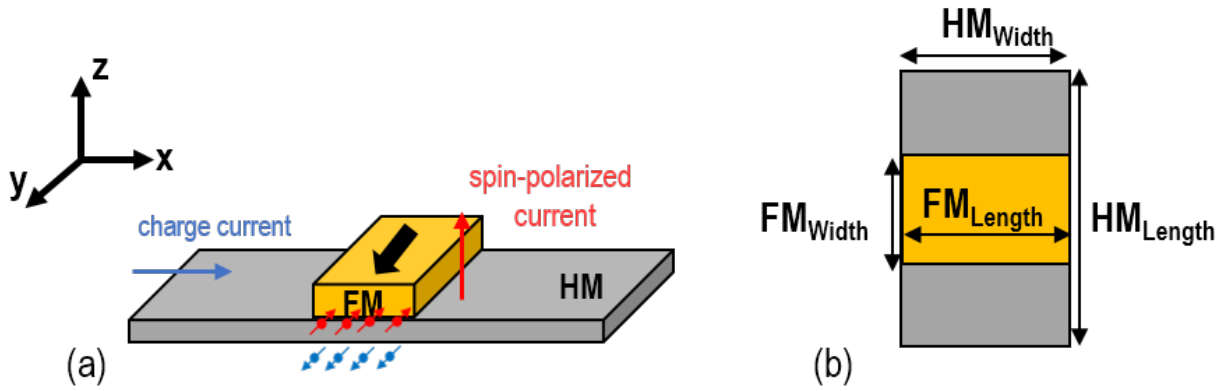


Figure 2.9: (a) Positive current along +x induces a spin injection current +z direction. The injected spin current produces the required spin torque for aligning the magnetic direction of the FM in +y directions, (b) Top view.

Non-volatile spin-based logic

The potential of spin-based memories such as STT-MRAM is relatively well known, whereas realizing logic remains an open challenge. There are several magnetic-based logic architectures have been proposed, such as Magnetic Quantum-dot Cellular Automata (MQCA) [2, 64, 65, 66], Domain Wall Logic (DWL) [3, 67], All-Spin-Logic (ASL) [4, 68], and MTJ-based logics [69, 70, 5], as shown in Figure 2.10. MQCA consists of multiple nanomagnets located closely and operates based on the states of applied inputs. DWL uses domain wall to store and compute information. ASL stores information using the spin of electrons of magnets and propagate the state using spin-polarized currents. MTJ-based designs are similar to MRAM in functionalities [5]. For all the architectures, magnetic field or spin-polarized current is utilized. Table 2.1 summarizes strength/limitation characteristics of the highly-used spin-based devices relative to CMOS.

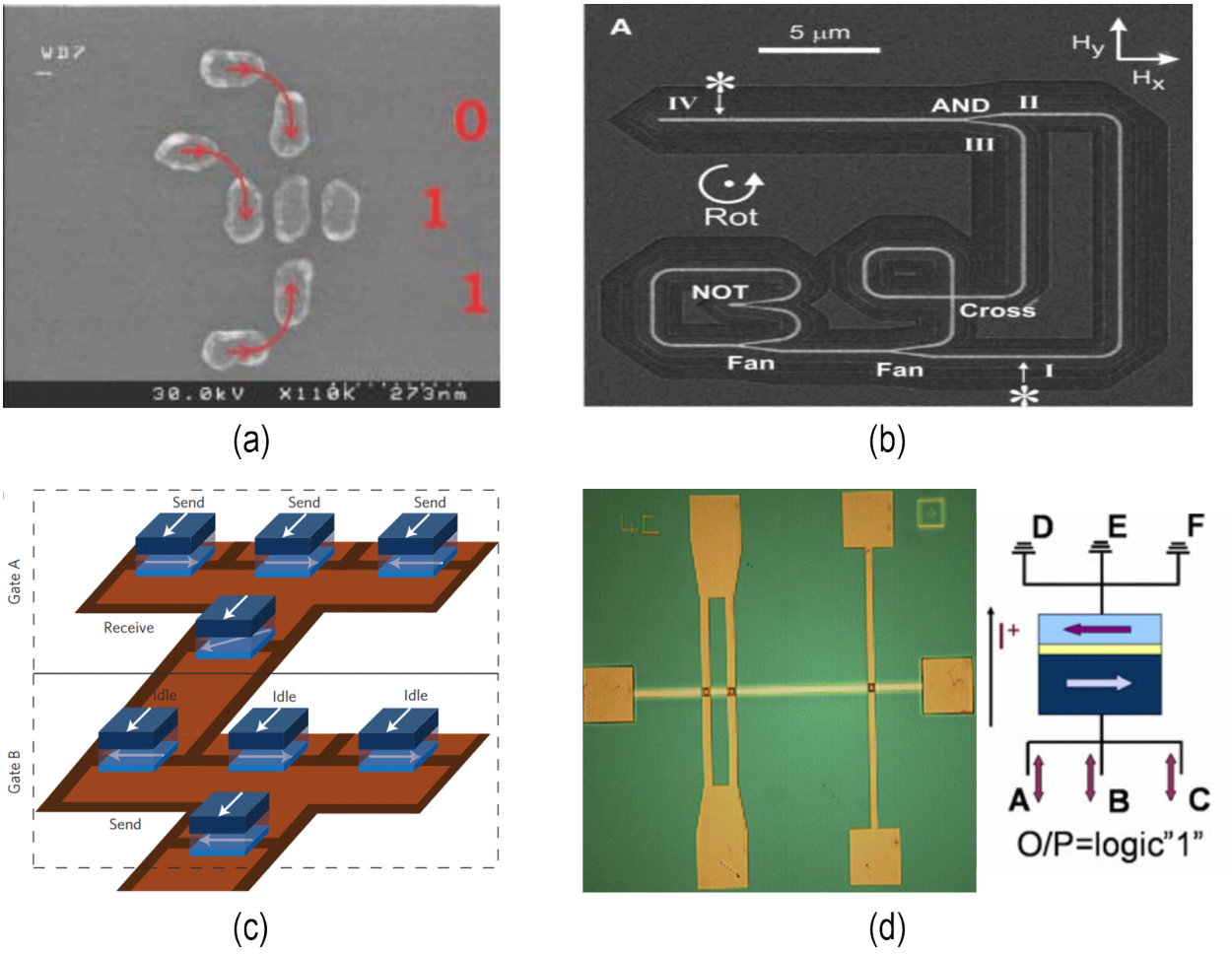


Figure 2.10: Main magnetic logic architectures, (a) MQCA [2], (b) DWL [3], (c) ASL [4], and (d) MTJ-based logic cell [5, 6].

Intermittent Approaches

Table 2.2 lists some of the prior efforts addressing the intermittency challenge facing energy-harvesting-powered designs. In [71, 72], a traditional *checkpointing* approach is utilized to ensure the accurate forward progress of computation, whereby any volatile execution context is proac-

tively preserved in Non-Volatile Memory (NVM) prior to anticipated periods of power failure. A checkpointing approach may suffer from internal and external inconsistencies after each power loss. Internal inconsistency occurs when the execution context is partially-retained in NVM, while external inconsistency arises when the power failure occurs between two checkpoints [73]. DINO [74] innovated a checkpointing-based approach that utilizes non-volatile versioning to retain memory consistency, as delineated in Table 2.2.

Table 2.1: Characteristics of enabling technologies. "✓" or "-" indicates strength/limitation relative to CMOS.

Technology / **Attributes**		**CMOS**	**MTJ**	**SHE**	**DWL**	**ASL**	**NML**
Power	Static	0	✓✓	✓✓	✓✓	✓✓	✓✓
	Dynamic	0	-	-	-	-	-
	Write	0	-	0	-	-	-
Memory		0	✓	✓	✓	-	-
logic		0	-	-	-	✓	✓
Density		0	✓	✓	✓	✓	✓✓
Speed		0	-		–	-	-
Reliability		0	✓	✓✓	✓	-	-

Duty Cycling with Scheduling [75, 76] offers another approach for tolerating intermittence. In this method, critical states of the processor will be partially-retained before the power failure, then the device will enter an extremely-low power mode. However, this results in full availability of the device only when a power interruption is unlikely, which can incur relatively long sleeping periods due to the inevitable power outages in many energy harvesting-powered systems. Chain [77] is another model for programming intermittent devices, in which forward-progress is ensured at the task granularity level. It utilizes *idempotent processing* concepts to make tasks restartable that never experience inconsistency to keep NVM consistent. In [32], a Non-Volatile MIPS Processor (NVP) is introduced in which specific blocks such as register files and pipeline registers were replaced by non-volatile elements. As listed in the last row of Table 2.2, NVP utilizes a checkpointing

approach to retain the processor volatile states resulting in possible above-mentioned internal and external inconsistencies in non-volatile elements. Advancing beyond previous intermittent processors which utilize NVM resources that are distinct from the processing datapath, we propose a new paradigm for energy-harvesting-powered processing, referred to as *Elastic Intermittent Computing* (EIC).

Table 2.2: Selected previous works with significant contributions towards intermittent processor design.

Approach	**Methodology**	**Features**	**Robust Element**	**Challenges**
Mementos [71]	checkpointing	Run-time energy estimation Periodic system snapshots 340 Byte footprint illustrated VON = 4.5V, VOFF = 2V	Flash	New programming paradigms and Languages Data movement overhead Low endurance
Hibernus [75]	duty-cycling reactive hibernating	Snapshot before outage 76%-100% less processing time and 49%-79% lower energy overhead than Mementos	Ferroelectric RAM (FRAM)	NVMs to save all processor register/states Need for sufficient energy to save a full snapshot Long sleeping time
DINO [74]	Checkpointing Data versioning	582 Byte footprint illustrated Atomic tasks Reduced flow complexity	Ferroelectric RAM (FRAM)	Large NVM versioning info New programming paradigm Data movement $\sim$4KB average storage overhead
Chain [77]	task-based control flow Channel-based memory model	Idempotent tasks; no checkpoints 2x to 7.6x performance compared to DINO	Ferroelectric RAM (FRAM)	Hardware redundancy New programming paradigms 42% larger code than DINO $\sim$8KB average storage overhead
NVP [32]	PC/register store Partial backup	NV flip-flops in MIPS ISA 1 KHz square waveform 3 MHz clk; 470nF store capacitor	Ferroelectric RAM (FRAM)	Non-volatile internal and external coherence Overhead of checkpointing

CHAPTER 3: COMPACT MODEL OF STT/SHE FOR BOTH IMTJ AND PMTJ

As mentioned in previous chapters, spintronic devices show promising features such as non-volatility. Hence, in order to design, analyze and compare the performance of spin-based devices with previously proposed architectures, a compact model is required. Moreover, as presented in Chapter 2, STT/SHE MTJs are the most promising components for spin-based designs. Hence, in this chapter, a SPICE-compatible model for both STT-MTJ and SHE-MTJ is developed. A number of realistic material parameters and physical models have been integrated into the models to achieve good agreement with experimental measurements. Our model consists of two sub-models: (1) MTJ resistive behavior, and (2) STT switching model.

Compact Model Of STT-MTJ

We considered NiFe/MgO and CoFeB/MgO stack for IMTJ and PMTJ, respectively, to gain the best performance of write and read operations.

MTJ Resistive Model

The tunneling conductance of barriers was proposed in [78], in which the conductance is voltage-dependent. [78] shows that the resistive behavior for this kind of structure, two ferromagnetic layers separated by a trapezoidal barrier, depends on its oxide barrier height and the effects between these layers. To simplify the proposed approximation, we considered that the oxide barrier is symmetric. Hence, simplified equations which are integrated into our model to calculate the

resistance of the MTJ are expressed as below [79]:

$$R_{MTJ} = \frac{t_{ox}}{Factor \times Area\sqrt{\phi}}.exp(1.025 \times t_{ox}\sqrt{\phi}) \tag{3.1}$$

where t_{ox} is the oxide thickness of MTJ, $Factor$ is obtained from the resistance-area product value of the MTJ that relies on the material composition of its layers, $Area$ is the surface of MTJ, and ϕ is the oxide layer energy barrier height. The energy barrier between P and AP configurations of MTJ is in a range such that it can switch between configurations, while also retaining thermal stability. The energy barrier for IMTJ and PMTJ are expressed by the following equations [80]:

$$E_{IMTJ} = \frac{\mu_0 M_s V H_C}{2} \tag{3.2}$$

$$E_{PMTJ} = \frac{\mu_0 M_s V H_K}{2} \tag{3.3}$$

The V is the volume of the free layer, Ms is the saturation magnetization, H_C is the in-plane coercive field, and H_K is the perpendicular magnetic anisotropy field. Since H_K is higher than H_C, PMTJ provides high energy barrier which leads to higher thermal stability.

There are two different magnetization configurations for ferromagnetic layers, parallel (P) and antiparallel (AP), according to which MTJ resistance changes between RP and RAP, respectively. MTJ resistance is determined by the angle (θ) between the magnetization orientations of the fixed layer and free layer due to the tunnel magnetoresistance (TMR) effect. As previously mentioned, TMR is the primary aspect to perform the reading operation. In order to decrease read disturbance, in our design, TMR ration is set to 100% and 120%. In our model, we determine RMTJ as the resistance of the RP. The MTJ resistance in P (θ=0°), and AP (θ=180°) states is obtained and

expressed by the Equation 3.4 [81].

$$\begin{cases} R(\theta) = 2R_{MTJ} \times \dfrac{1+TMR}{2+TMR+TMR.cos\theta} \\ TMR = TMR(0)/1 + (\dfrac{V_b}{V_h})^2 \end{cases} \tag{3.4}$$

where V_b is the bias voltage, and V_h = 0.5V is the bias voltage when TMR is half of the TMR_0. Figure 3.1 depicts a large resistance hysteresis of an MTJ by sweeping the bias voltage, which makes MTJ-based devices suitable for non-volatile designs.

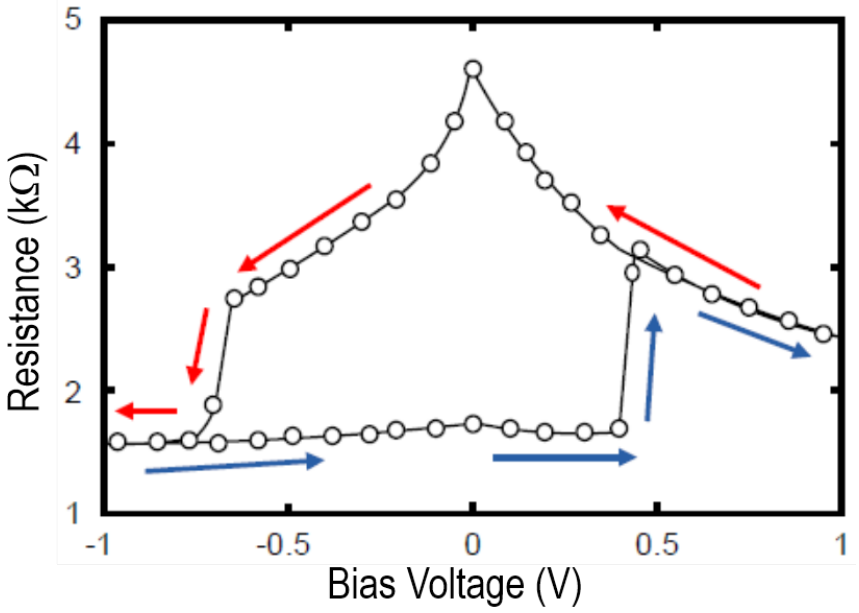


Figure 3.1: Resistance hysteresis of an MTJ, red arrow shows switching from AP to P, while blue arrow indicates switching from P to AP.

Spin-Transfer Torque (STT) Switching Model

Herein, first, we explain the required critical current for both MTJ types and then use them to calculate the switching delay for switching between P and AP states. As aforementioned, the magnetic direction of MTJ layers can be in the film plane, IMTJ (in-plane MT), or PMTJ (out of the film plane referred to as perpendicular MTJ) structure, as shown in Figure 3.2 (a) and (b), respectively. Equations 3.5 and 3.6 express the switching critical current for IMTJ [82] and PMTJ [83], respectively.

$$I_{c-IMTJ} = \frac{2\alpha e M_s V \left(H_c + \frac{H_{eff}}{2}\right)}{g(\theta) P \hbar} \tag{3.5}$$

$$I_{c-PMTJ} = \frac{\alpha \gamma e M_s V H_K}{\mu_B g(\theta)} \tag{3.6}$$

The parameter α is the magnetic damping constant, μ_B is the Bohr magneton, P is the spin polarization percentage of the tunnel current, γ is the gyromagnetic ratio, e is the electric charge, $\hbar$ is the reduced Planck's constant, and H_{eff} is the effective out-of-plane demagnetization field, which consists of external field, in-plane uniaxial magnetic anisotropy field, and out-of-plane magnetic anisotropy. The effective demagnetization field in IMTJ is approximately equal to the saturation magnetization, which is normally larger than the anisotropy field in PMTJ. Thus, switching current for PMA is smaller than that of the IMA devices. Moreover, spin polarization efficiency factor, $g(\theta)$, is a function of the angle between the free layer and fixed layer magnetization directions (θ) and is obtained by the Equations 3.7 and 3.8 [83] for IMTJ and PMTJ devices, respectively.

$$\begin{aligned} g_{IMTJ} &= \Big[-4 + \frac{(P^{-1/2} + P^{1/2}) \times (3 + cos\theta)}{4} \Big]^{-1} \\ g_{PMTJ} &= g_{SV} \pm g_{tunnel} \end{aligned} \tag{3.7}$$

$$g_{SV} = \Big[-4 + \frac{(P^{-1/2} + P^{1/2})^3 \times (3 + cos\theta)}{4} \Big]^{-1}$$
$$g_{tunnel} = \frac{P}{2(1 + P^2 cos\theta)} \tag{3.8}$$

where g_{SV} is the spin polarization efficiency in a spin valve and g_{tunnel} is the spin polarization efficiency in tunnel junction nanopillars.

As explained in previous chapters, based on the STT approach, a bidirectional spin-polarized current (I_{MTJ}) is required for switching MTJ nanomagnet configuration, as shown in Figure 3.2. Electrons that flow through the MTJ free layer will experience an exchange field which aligns the spin of the electron with the magnetization direction of the nanomagnet. This phenomenon is called spin-filtering effect. The conservation of the angular momentum results in the exertion of an opposite sign torque with the equal magnitude on the free layer which eventually changes its magnetization direction. The P or AP configuration of the MTJ is determined by the direction of the current that flows through it. The required bidirectional current could be produced by means of simple MOS-based circuits. Due to the vertical structure of the MTJ, it can be readily integrated at the back-end process of the CMOS fabrication [84, 12]. According to the relative amplitude of the IMTJ and the switching critical current (I_C), STT switching behavior can be categorized into two main regions: (1) precessional region (I_{MTJ} I_C), and (2) thermal activation region (I_{MTJ} łI_C) which are described by Sun model [85] and Neél-Brown model [86], respectively.

In the precessional region, MTJ experiences rapid precessional switching. Equation 3.9 describes the switching duration of the MTJ in this region[84].

$$\frac{1}{\langle \tau_{STT} \rangle} = \Big[\frac{2}{C + ln(\pi^2 \Delta)} \Big] \frac{\mu_B P}{em(1 + P^2)} (I_{MTJ} - I_C) \tag{3.9}$$

where τ_{STT} is the mean duration for the precessional switching region, C=0.577 is the Euler's constant, $\Delta = E/(4k_BT)$ is the thermal stability factor, and m is the free layer magnetic moment. In the thermal activation region, although the current is less than the critical value, the switching can occur with a long input current pulse due to the thermal activation. The switching duration in the thermal activation region is described by the below equation [84]:

$$\frac{1}{\langle \tau_{STT} \rangle} = \tau_0 exp\left(\Delta \times \left(-\frac{I_{MTJ}}{I_C}\right)\right) \tag{3.10}$$

where τ_{STT} is the mean pulse duration for the thermal activation region, and tau_0 is the attempt period. In practice, in order to have high switching speed, MTJ is required to work in the precessional region with a current amplitude larger than critical current.

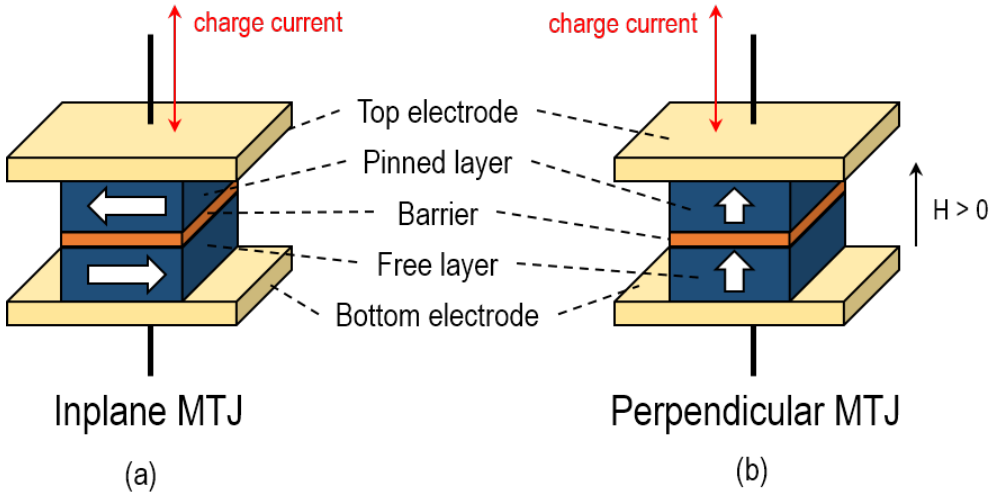


Figure 3.2: Illustrations (a) in-plane and (b) out-of-plane or perpendicular magnetized MTJ.

STT-MTJ Based Look-Up Table

To validate our develop STT-MTJ model, a four-input STT-LUT, as shown in Figure 3.3, is introduced and its functionality is verified. It consists of read and write circuits. The write circuit includes two transmission gates (TGs), which provide the desired charge current for STT switching, whereas the read circuit is composed of a pre-charge sense amplifier (SA) [47], a TG-based multiplexer (MUX), and a reference tree. Each MTJ cell of LUT could be accessed according to the input signals A, B, C, and D, through MUX, which employs TGs instead of pass transistors (PTs). LUT is utilized in reconfigurable fabrics to implement combinational logic. In general, LUT is a memory with 2^m cells in which the truth table of an m-input Boolean function is stored. Inputs can be considered as the address according to which corresponding output of the Boolean function will be returned.

The reference tree in read circuit is designed to provide SA with required reference resistance to properly sense each MTJ cell state. The reference tree consists of four TGs in a series configuration to compensate for the select tree active resistance. Reference MTJ resistance is designed in a manner such that its value in the parallel configuration is between low resistance, i.e., R_P , and high resistance, i.e., R_{AP}, of the LUT MTJ cells, as shown in the following equation:

$$R_{P-referenceMTJ} \cong \frac{1}{2}(R_P + A_{AP}) \tag{3.11}$$

According to Equation 3.4, the resistance of MTJ can be altered by changing t_{ox} or Area. Oxide thickness could be only changed between 0.7 and 2.5 nm to keep the low-resistance value and show the TMR effect. Additionally, as established in [87], fabricating MTJs with various oxide thicknesses requires different magnetic processes, which leads to a significant increase in fabrication cost.

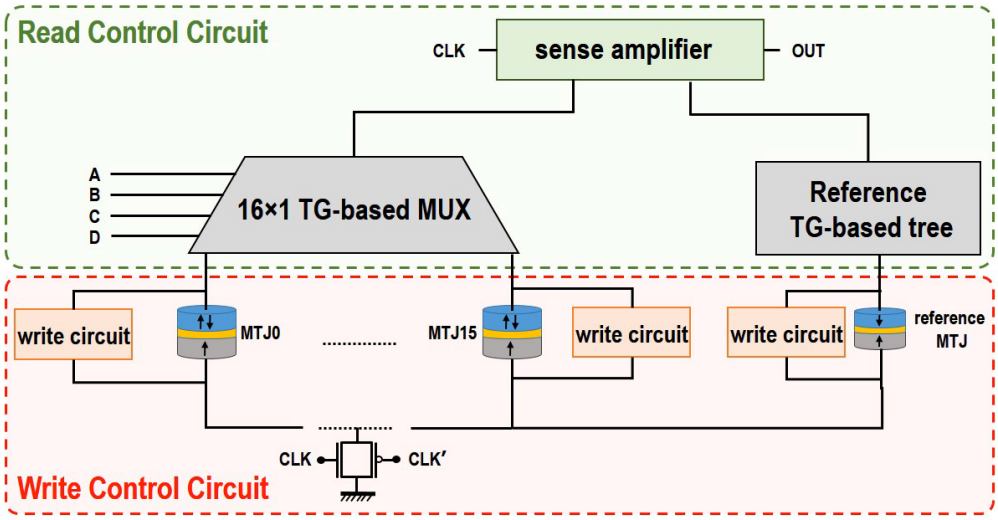


Figure 3.3: Four-input STT-LUT functional diagram.

Thus, in this brief, the other effective factor, i.e., Area, is examined to determine the desired value of reference MTJ resistance. The dimensions of LUT and reference MTJ cells are shown in Figure 3.4, according to which $R_{PreferenceMTJ}$, R_{AP}, and R_P are equal to 1.8, 2.5, and 1.25 kΩ, respectively. The proposed design is simulated for LUTs with different numbers of inputs using SPICE simulator in 90-nm library. Delay and power consumption results are summarized in Table 3.1. As listed in the table, power and delay of STT-LUT are larger [88] when the MTJ state is P, due to the inequality shown in the following equation, which results in a longer time required for SA to be completely discharged:

$$R_{AP} - R_{P-referenceMTJ} > R_{P-referenceMTJ} - R_P \tag{3.12}$$

Herein, the developed STT-LUT circuit is implemented utilizing both PTs and TGs. The performances of our STT-LUT implementations are compared with SRAM-LUT [89] and two afore-

mentioned MTJ-based LUTs and summarized in Tables 3.1 and 3.2, respectively. The STT-LUT provides high-speed and ultra-low power circuits with improved PDP values, shown in the seventh row in Table 3.2. Furthermore, TG-based STT-LUT exhibits least PDP value while it leverages a larger number of MOS transistors compared with PT-based STT-LUT, which is the optimum choice from the area efficiency point of view.

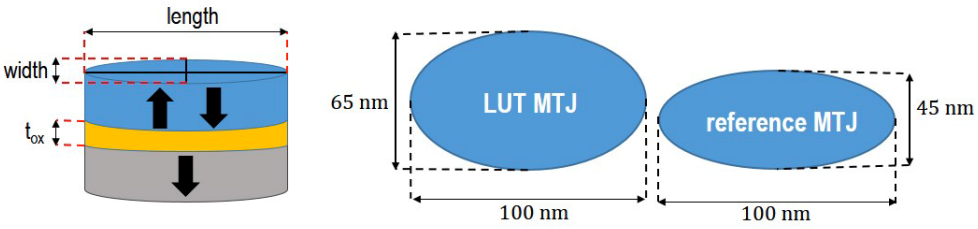


Figure 3.4: Reference MTJ cell and LUT MTJ cell dimensions.

Table 3.1: performance comparison between STT-LUT and SRAM-LUT for four-input NAND operation.

Parameter		SRAM-LUT [89]	PT-based STT-LUT [48]	TG-based STT-LUT [48]
Area		14.3×16.55	7.2×8.35	13.5×15.75
Power Consumption ()	Leakage	1.030	0	0
	Dynamic	1.217	4.30	4.27
	Total	2.247	4.30	4.27
Delay (ps)		85.86	94	83

Figure 3.5 elaborates the functionality of the proposed STT-LUT for a four-input NAND operation when ABCD = “1111” and ABCD = “0000” inputs are applied. The former set of inputs selects MTJ15, which has a parallel configuration that denotes logic “0”, whereas the latter input selects MTJ0 with antiparallel configuration representing logic “1”.

Table 3.2: Performance comparison for four-input NAND operation.

Features	Zhao [90]	Suzuki [91]	PT-based STT-LUT[48]	TG-based STT-LUT [48]
NO. of MTJs	32	36	17	17
NO. of MOSs	154	74	59	112
Delay (ps)	88	81	94	83
Active Power (μW)	13.40	7.58	4.30	4.27
PDP (p$\times$ μW)	1179.2	613.98	404.20	354.41
Standby Power	0	0	0	0
PDP	-	48%	65.7%	70%
Improvement	-	-	34%	42%

While STT approach offers significant advantages in terms of read energy and speed, a significant incubation delay due to the pre-switching oscillation [16, 17] incurs high switching energy. Hence, to achieve a high-speed write operation, we can enlarge the write transistor width, or/and reduce the critical current. The former one leads to large area overhead and also increases risk of MTJ barrier breakdown. While the latter solution decreases the thermal stability. Recently, SHE-MTJ is introduced as an alternative for 2-terminal MTJs, which provides separate paths for read and write operations, while expending significantly less switching energy [18, 19, 20].

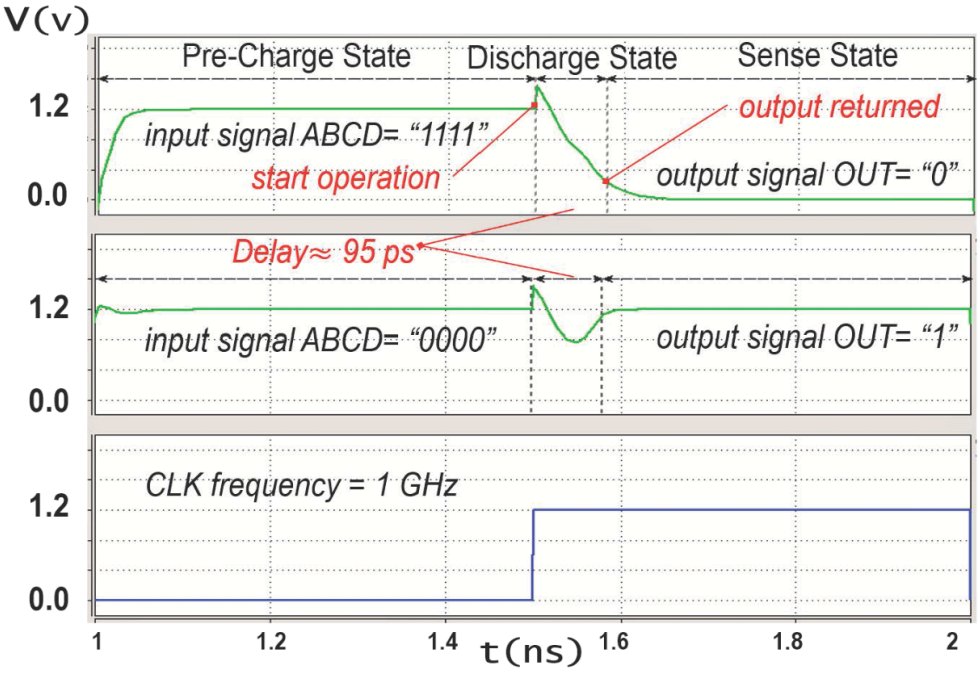


Figure 3.5: Transient response of STT-LUT for four-input NAND operation for (top) ABCD = "1111" and (middle) ABCD = "0000".

Compact Model Of SHE-MTJ

As mentioned, spin-polarized currents can be utilized to generate the torque required for switching the magnetization directions of the free layer in MTJs. It is shown in [1] that spin current can be produced in nanomagnetic devices by the spin-Hall effect. In [19], Manipatruni et al. have provided the physical equations of the three-terminal SHE-MTJ device behavior. Figure 3.6 shows the structure of the SHE-MTJ device, in which the magnetic orientation of the free layer changes by passing a charge current through a heavy metal (HM). MTJ free layer is directly connected to HM which is normally made of β-tantalum (β-Ta) [1], β-tungsten (β -W) [62] or Pt [63]. The MTJ

logic state that is defined by the free layer magnetic direction is determined by the direction of the applied charge current. The spin-orbit coupling in HM deflects the electrons with different spins in opposite directions, which results in a spin injection current transverse to the applied charge current. The injected current produces the required spin torque for aligning the magnetic direction of the free layer.

Ratio of the injected spin current to the applied charge current, called spin Hall injection efficiency (SHIE), is defined by Equation 3.13:

$$SHIE = \frac{I_{sz}}{I_{Icx}} = \frac{\pi . MTJ_{width}}{2HM_{thickness}} \theta_{SHE} \left[1 - sech\left(\frac{HM_{thickness}}{\lambda_{sf}} \right) \right] \tag{3.13}$$

where MTJ_{width} is the width of the MTJ, $HM_{thickness}$ is the thickness of the HM, λ_{sf} is the spin flip length in HM, and θ_{SHE} is the SHE angle [19]. This equation is valid for SHE-MTJ devices in which the length of the MTJ equals the width of the HM.

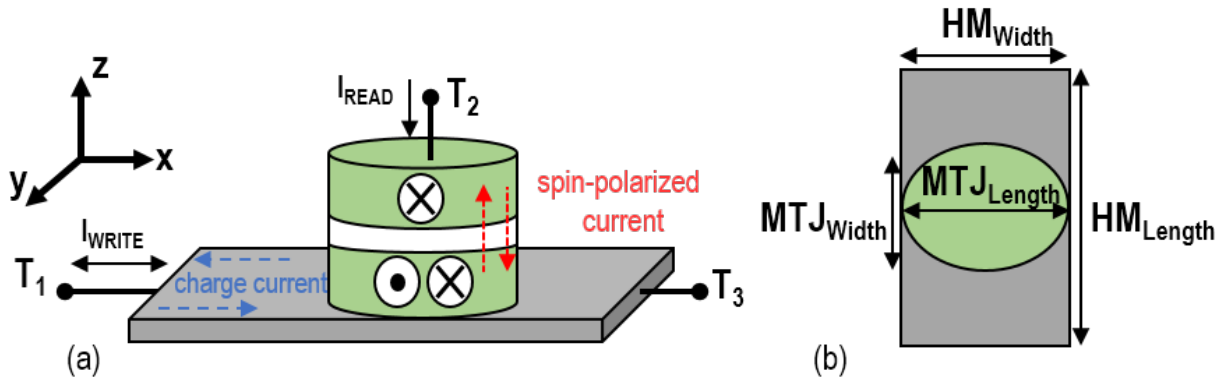


Figure 3.6: SHE-MTJ vertical structure. Positive current along +x induces a spin injection current +z direction. The injected spin current produces the required spin torque for aligning the magnetic direction of the free layer in +y directions, and vice versa. (b) SHE-MTJ Top view.

Herein, SHIE value is equal to 1.73 that is extracted using Equation 3.13. Thus, the generated spin current is larger than the applied charge current. Whereas the spin injection efficiency of a 2-terminal MTJ (STT-MTJ) is normally less than one resulting in a favorable write switching energy for SHE-MTJs used in LUTs herein, as quantified by Equation 3.13. The critical spin current required for switching the free layer magnetization orientation is expressed by Equation 3.14:

$$I_{s,critical} = \frac{2q\alpha M_S V_{MTJ}(H_k + 2\pi M_S)}{\hbar} \tag{3.14}$$

where VMTJ is the MTJ free layer volume. Thus, SHE-MTJ critical charge current can be calculated using Equations 3.13 and 3.14. Equation 3.15 shows the relation between SHE-MTJ switching time and the voltage applied to the HM terminals with the critical voltage v_c given by Equation 3.16 [19].

$$\tau_{SHE} = \frac{\tau_0 ln(\pi/2\theta_0)}{(\frac{v}{v_c}) - 1} \tag{3.15}$$

$$v_c = 8\rho I_c \left\{ \theta_{SHE} \left[1 - sech\left(\frac{HM_{thickness}}{\lambda_{sf}}\right) \right]_{length} \right\}^{-1} \tag{3.16}$$

where, $\theta_0 = \sqrt{k_B/2E_b}$ is the effect of stochastic variation, E_b is the thermal barrier of the magnet of volume V, HM_{length} is the length of the HM, and I_c is the critical charge current for spin-torque induced switching. In order to model the SHE-MTJ, the HM resistance is also required, which is expressed by Equation 3.17, where ρ_{HM} is the electrical resistivity of HM.

$$R_{HM} = \frac{\rho_{HM} \times HM_{length}}{HM_{width} \times HM_{thickness}} \tag{3.17}$$

Verilog-AMS is utilized to model the behavior of SHE-MTJ devices based on the aforementioned physical equations. Then, the model is leveraged in SPICE circuit simulator to validate the functionality of the designed circuits using experimental parameters listed in Table 3.3.

Figure 3.7 (a) and 3.7 (b) show the MOS-based bit-cell of the 2-terminal MTJ (STT-MTJ) and 3-terminal MTJ (SHE-MTJ), respectively. In SHE-MTJ, the spin current can be significantly larger than the applied charge current. Therefore, the transistor utilized in the bit-cell of the STT-MTJ should be larger than that of the SHE-MTJ to be able to provide equal switching delay. Thus, although SHE-MTJ bit-cell requires two MOS transistors, its integration density is comparable to the STT-MTJs.

Table 3.3: Parameters of SHE-MTJ-based LUT.

Parameter	**Description**	**Value**
HM Volume	$HM_{Length} \times HM_{Width} \times HM_{Thickness}$	100×60×3 nm^3
MTJ Area	$MTJ_{Length} \times HM_{Width} \times \pi/4$	60×30×$\pi/4$ nm^2
MTJ Area	Reference MTJ Surface	50×25×$\pi/4$ nm^3
$I_{C\text{-}SHE}$	SHE-MTJ Critical Curren	108 μA
$I_{P\text{-}AP}$	STT-MTJ Critical Current for P to AP Switching	37 μA
$I_{AP\text{-}P}$	STT-MTJ Critical Current for AP to P Switching	18 μA
θ_{SHE}	Spin Hall Angle	0.3
ρ_{HM}	Resistivity	200 $\mu\Omega.cm$
ϕ	Potential Barrier Height	0.4 V
t_{ox}	Thickness of oxide barrier	0.85 nm
α	Gilbert Damping factor	0.007
M_s	Saturation magnetization	200 7.8e5 $A.m^{-1}$
μ_B	Bohr Magneton	9.27 e-24 $J.T^{-1}$
P	Spin Polarization	0.52
γ	Gyromagnetic Ratio	1.76e7 $(Oe.s)^{-1}$
R_{AP}, R_P	MTJ Resistances	2.8 KΩ, 5.6 KΩ
R_P	Reference MTJ Resistance	4.12 KΩ
TMR_0	TMR ratio	4.12 100%
H_k	Anisotropy Field	80 Oe
μ_0	Permeability of Free Space	1.25663e-6 T.m/A
θ_{SHE}	Spin Hall Angle	0.3
ρ_{HM}	HM Resistivity	200 $\mu\Omega$.cm
ϕ	Potential Barrier Height	0.4 V
Λ_{sf}	Spin Flip Length	1.5nm
e	Electric charge	1.602e-19 C
$\hbar$	Reduced Planck's Constant	6.626e-34/2π J.s

Increasing the transistor size in STT-MTJs may also result in occasional read/write disturbances due to a common read/write path. Moreover, the reliability of the tunneling oxide barrier is improved in SHE-MTJ, since the current does not flow through it during the write operation. Table 3.4 provides a comparison between the STT and SHE write schemes in terms of the switching delay and energy consumption for a single MTJ cell. Assuming the typical 50% duty cycle, the maximum operating clock frequency based on which each of the circuits can ensure complete switching of the MTJ states is listed in Table 3.4. We have examined the SHE-LUT reconfiguration energy according to the clocking requirements illustrated in Table 3.4.

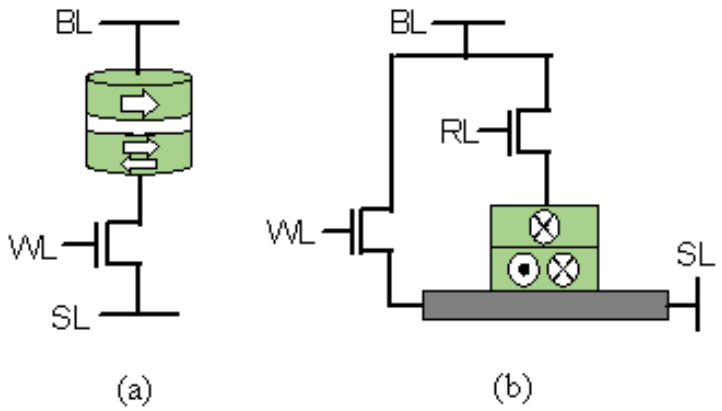


Figure 3.7: (a) 2-terminal MTJ (STT-MTJ) bit-cell, (b) 3-terminal (SHE-MTJ) bit-cell.

Table 3.4: Switching Characteristics of a Single MTJ Cell Including Clocking Requirements.

Features		STT-MTJ	SHE-MTJ
Switching	P to AP	3.3	1.98
Delay (ns)	AP to P	3.37	1.96
Maximum CLK Frequency		140 MHz	250 MHz
Switching	P to AP	521.2	361.7
Energy (fJ)	AP to P	400.2	362.7

SHE-MTJ Based Look-Up Table

Herein, a non-volatile LUT circuit is developed based on the SHE-MTJ devices introduced in the previous section. As shown in Figure 3.8, SHE-LUT structure includes two main parts: write circuit and read circuit. Designing the read and write circuits requires considering important details which can significantly influence the energy consumption and delay of the LUT circuit.

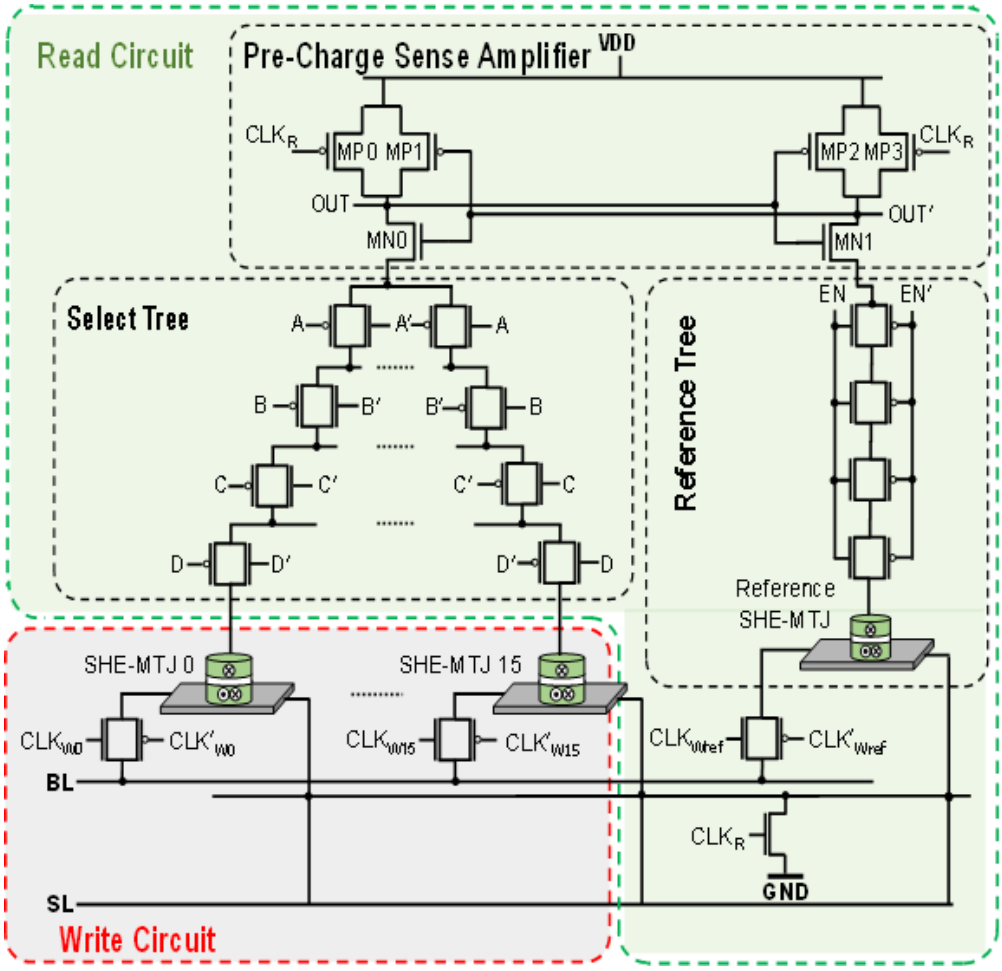


Figure 3.8: Circuit-level design of proposed SHE-LUT.

The select tree in the read circuit enables accessing each of the storage cells in LUT according to

the address provided by A, B, C, and D input signals. Pass Transistors (PTs) and Transmission Gates (TGs) have been investigated in [48, 92] to be utilized in the LUT select tree. Results exhibited that TG-based select tree has lower propagation delay and more resiliency to process variation compared with PT-based select tree while consuming relatively equal power. Therefore, herein TG-based select tree is utilized in our proposed SHE-LUT, as shown in Figure 3.8. In this design, we have utilized SHE-MTJ as a storage element in the LUT circuit. In general, data is stored in resistive memory cells in the form of different resistance levels, e.g. high resistance state stands for logic 1 and vice versa. Therefore, a sense amplifier (SA) is required to distinguish the resistive state of the memory cell. In [47], Zhao et al. studied various SAs which could be leveraged for sensing the magnetic configuration of the MTJs. They have proposed a Pre-Charge Sense Amplifier (PCSA) consisting of seven MOS transistors and a reference MTJ, which could provide a low power and high speed read operation while maintaining a low error rate. Moreover, a TG-based reference tree including four TGs in the series configuration is utilized in our designs to compensate for the select tree resistance. Reference MTJ dimensions are designed in a manner such that its resistance value in the parallel configuration is between low resistance, R_{Low}, and high resistance, R_{High}, of the SHE-based MTJ cells as elaborated by below equations:

$$\begin{aligned} R_{P-referenceMTJ} \cong \frac{1}{2}(R_{Low} + R_{High}) = \frac{R_{AP-LUTMTJ} + R_{P-LUTMTJ}}{2} + \frac{R_{HM}}{2} \\ R_{Low} = \left(R_{P-LUTMTJ} + \frac{R_{HM}}{2}\right) \quad and \quad R_{High} = \left(R_{AP-LUTMTJ} + \frac{R_{HM}}{2}\right) \end{aligned} \tag{3.18}$$

We have utilized a TG in the SHE-MTJ write circuit, as shown in Figure 3.8. TGs are composed of one NMOS and one PMOS transistor, and characterized by their near optimal full-swing switching behavior. TG-based write circuit provides a symmetric switching behavior, i.e. the generated write current amplitude for P to AP switching equals the current amplitude produced for switching from AP to P state. Moreover, TGs are capable of producing a current amplitude larger than the switching critical currents of both STT-MTJ and SHE-MTJ devices.

Table 3.5: Performance comparison for the Reconfiguration Operation of 4-input MTJ-LUTs Involving 16 MTJs.

Features		STT-MTJ Based LUT [[48]]	SHE-MTJ Based LUT [[49]]
Delay (ns)	P to AP	52.8	31.68
	AP to P	53.92	31.36
Power Consumption (mW)	P to AP	1.16	1.44
	AP to P	0.89	1.45
PDP (ns$\times$ mW)	P to AP	3.83	2.85
	AP to P	3.30	2.84
Average PDP (ns$\times$ mW)		3.565	2.845
Average PDP Improvement		20.1%	-

Table 3.5 provides a comparison between the reconfiguration operation of a 4-input SHE-LUT and a conventional MTJ-LUT. A 4-input MTJ-LUT includes sixteen MTJs having their magnetization directions aligned in a single reconfiguration operation. As listed in Table 3.5, the proposed SHE-LUT provided at least 20% PDP improvement compared to STT-MTJ LUTs. The clocking limitations in reconfigurable fabrics may change the results provided in Table 3.5.

CHAPTER 4: SPINTRONICS MAJORITY GATE BASED DESIGNS

As it can clearly be perceived, the unifying computational mechanism underlying all of these TMR-based devices is an accumulation-mode operation that enables the realization of majority logic functions as basic computational building blocks [4, 93]. Therefore, first, we developed an MG-based synthesis and optimization research tool and then based on its results we design a 1-bit majority gate (MG)-based full adder, which is one of the most important functional building blocks.

MG-based Synthesis and Optimization Research Tool

This section focuses on implementing Boolean gates and logic circuits based on the MGs. To achieve this objective, we develop an MG-based synthesis and optimization routine and tool. In our approach, Genetic Algorithm (GA) has been used to design logic circuit networks which are implemented by majority gates.

GAs are optimization tools inspired by the nature that simulate the natural selection process to find the solutions to optimization problems. These algorithms are one of the most popular optimization tools due to their ability to optimize any objective function regardless of the gradient or higher derivatives of the objective function. Problems of logic optimization for digital designs are complicated problems on their own that also usually suffer from lack of derivable or even continuous functions that are able to present them. Therefore, GA has been chosen in such problems as an excellent choice. In the following the main parts of a typical GA has been briefly explained.

Initialization: the GA starts with creating an initial set (population) of solutions (chromosome) to the problem, called the initial population. The population size and the initial population variety

should be considered in a way that the GA be able to achieve acceptable solutions in a reasonable time. It should be considered that extending the population size leads to increasing the variety of chromosomes, of course, this relationship is limited to some upper bound, but this extension also leads to the increase in the total processing time of the GA.

Fitness Evaluation: GA in order to be able to direct the population to better solutions, should evaluate each chromosome. The evaluation of chromosome is carried out using the fitness function that assign a value to a chromosome based on how far or close it is from the solution. This evaluation occurs many times in the execution of the algorithm, such as when the parent selection is required, or when some individuals (chromosomes) should be selected to constitute the next generation population.

Parent Selection: each chromosome with a probability proportional to its fitness value can participate in the reproduction of new chromosomes. Regardless of the way that we correspond the fitness value of a chromosome to its probability of being selected as a parent, a portion of the population should be selected to reproduce by way of the crossover operator and another portion of the population should be selected to reproduce by way of the mutation operator.

Crossover Operator: the role of crossover operator in the GA is to generate new offspring(s) from the selected parents according to a probability in order to achieve new solutions to the problem. The number of the parents that participate in the generation of the offspring and how the offspring is generated by the application of this operator varies over different types the crossover operator.

Mutation Operator: although the crossover operator generates new solutions to the problem the GA is susceptible to stick in the local optima. The main role of the mutation operator is to help the GA escape the local optima and achieve global optima. This operator often applies on a chromosome and slightly changes it according to a probability in order to generate a new chromosome.

Replacement: after the new chromosomes being generated by way of crossover and mutation operators, these individuals in addition to some of the individuals in the current generation with the best fitness values make up the next generation.

This routine is repeated until some termination criterion is met, e.g., the algorithm reaches a defined number of generations.

In this chapter, the first version of the GA optimization unit has been developed, in which a combination of 3-input and 5-input MGs are considered as the primary building blocks in order to optimize the designs. This combination of majority gates includes either design based on only one type of MGs (3-input or 5-input) or designs including both types of the MG. The logical functions of 3-input MG and 5-input MG are as Equations 4.1. It expresses the output for an MG with n inputs, where n is always an odd number. The MG outputs "1" if and only if more than (n-1)/2 of the inputs are "1", and vice versa.

M(A,B,C) = AB + AC + BC

M(A,B,C,D,E) = ABC + ABD + ABE + ACD + ACE + ADE + BCD + BCE + BDE + CDE

(4.1)

A tree structure is used in order to represent the chromosomes Figure 4.1(a). In this structure, the root and the inner nodes of the tree are either a Majority or an Inverter specified with the Maj. and Inv. respectively. For example, M(A,D,C,1,B) is shown in Figure 4.1(b). The algorithm starts with a population including 500 chromosomes. So in order to both, 3- and 5- input MGs, of the effects be taken into account, a linear abstraction of fan-in as its cost function is considered, which has been defined as below:

$$f(C_i) = \frac{N(m, C_i)}{|m|} + \frac{1}{N(r, C_i)} + \frac{1}{Nodes(C_i)} \tag{4.2}$$

where $N(,)$ is a function that calculates the number of minterms in the first parameter implemented by the second one, m contains the minterms to be implemented, $|m|$ is the size of m and has been added for scaling issues, and r is the rest of minterms, that should not be implemented. The sub-tree crossover as a natural choice for tree shape chromosomes has been selected as the crossover operator that selects two nodes and exchanges their sub-trees rooted from the selected nodes. Mutation of a chromosome as performed in [94] is done by creating some randomly generated chromosomes and exchanging them by some other randomly selected chromosomes, proportional to a probability. The tournament selection has been utilized in order to select the parents for crossover and mutation operators. The algorithm stops when no improvement in fitness function happens during more than 20 generations or the total number of generations exceeds 1500.

To provide experimental evidence to study how the combination of 3-input and 5-input majority gates improves the performance of traditional design methods, the proposed optimization procedure is implemented in Python and results are illustrated in Table 4.1.

Table 4.1: Optimization of three standard functions.

Functions	Previous Works using 3MG	Proposed approach using combination of 3 and 5 MGs
1. BCD+ABC+ABD+ACD	**M**(B,C,**M**(D,A,0))	**M**(A,B,C,D,0)
2. $\overline{\mathrm{A}}.\overline{\mathrm{B}}.\overline{\mathrm{C}}$+ABC	**M**(**M**($\overline{\mathrm{C}}, A, 1$), **M**($C, B, 0$), $\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, 1)}$)	**M**(**M**(A,B,C,0,0),1,$\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{C}, 1, 1)}$)
3. A.B.C.D	**M**(**M**(A,B,0),0,**M**(0,C,D))	**M**(0,**M**(A,B,0),0,C,D)

Spintronics MG-based Circuit Designs

Binary addition is the most fundamental mathematical operation. It is worth mentioning that other operations in computer arithmetic such as subtraction and multiplication are usually implemented by adders and this importance has motivated alternative designs for adder (FA) structures. The

logic functions of the FA can be expressed as follows:

$$\begin{aligned} SUM &= A \oplus B \oplus C \\ C_{OUT} &= AB + AC + BC \end{aligned} \tag{4.3}$$

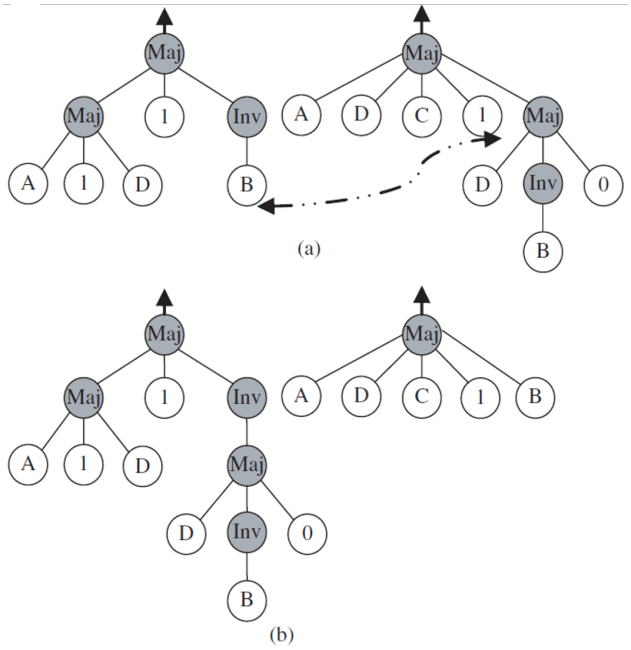


Figure 4.1: Two chromosomes (a) before crossover, and (b) after crossover.

The optimized MG-based 1-bit FA implementation using our developed GA-driven tool, as shown in Figure 4.2, is expressed as below:

$$\begin{aligned} C_{OUT} &= AB + AC + BC = 3 - inputMG(A,B,C) = \mathbf{M3}(A,B,C) \\ SUM &= M5(A,B,C,\overline{M3},\overline{M3}) = \mathbf{M5}(A,B,C,\overline{C_{OUT}},\overline{C_{OUT}}) \end{aligned} \tag{4.4}$$

We extracted the obtained SUM expression to prove the correctness of its functionality.

$$
\begin{aligned}
SUM &= M5(A,B,C,\overline{M3},\overline{M3}) = \mathbf{M5}(A,B,C,\overline{C_{OUT}},\overline{C_{OUT}}) \\
&= ABC + AB\overline{C_{OUT}} + AC\overline{C_{OUT}} + BC\overline{C_{OUT}} + A\overline{C_{OUT}} + B\overline{C_{OUT}} + C\overline{C_{OUT}} \\
&= ABC + \overline{C_{OUT}}(A+B+C) \\
&= ABC + (\overline{AB+AC+BC})(A+B+C) \\
&= ABC + (\overline{AB}\,.\,\overline{AC}\,.\,\overline{BC})(A+B+C) \\
&= ABC + \Big[(\overline{A}+\overline{B}).(\overline{A}+\overline{C}).(\overline{B}+\overline{C})\Big](A+B+C) \\
&= ABC + \overline{ABC} + \overline{A}B\overline{C} + A\overline{BC} = \mathbf{A}\oplus\mathbf{B}\oplus\mathbf{C}
\end{aligned}
\tag{4.5}
$$

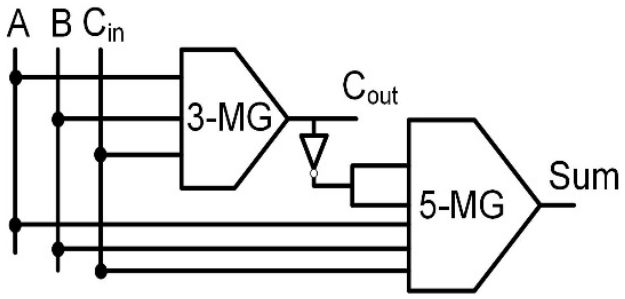


Figure 4.2: Schematic of a 1-bit full adder using 3- and 5- input MGs.

MG-based Full Adder using Current-Induced Domain Wall Nanomagnets

Leveraging the concept of FA schematic, as shown in Figure 4.2, our first spin-based circuit is a novel current mode FA design which is based on the Domain Wall NanoMagnet (DWNM) MGs. Current-Induced magnetic Domain Wall (CIDW) device is a transistor-less element, which leverages a new switching mechanism that has been proposed to overcome low-speed magnetic switching concerns. Each ferromagnetic domain can store a bit while each DW is a mobile interface

between regions of oppositely-aligned magnetization, which can be shifted laterally between two antiferromagnetic contacts by applying a current [95] as described below[1].

CIDW devices consist of a ferromagnetic nanowire in which opposite magnetic polarities form the Domain Walls (DWs) as shown in Figure 4.3. The DW can be moved within the nanowire according to the Spin Transfer Torque (STT) switching method utilizing an applied spin-polarized current [13]. The applied current only changes the orientation of the spin, thus DWs are not subjected to physical shift. A number of innovative proposals have been developed which use DWs in nanowires to denote the information bits for both memory [97] and logic devices [90, 67, 98]. Figure 4.4 (a) shows a DWNM device in which antiferromagnetic contacts are utilized at both its ends and fixed in antiparallel direction relative to each other to ensure the existence of a single DW in the device. To realize the writing operation of a single bit, a bidirectional current is used. The bit value of logic "0" is indicated upon shifting the DW to the left, and vice versa for logic "1".

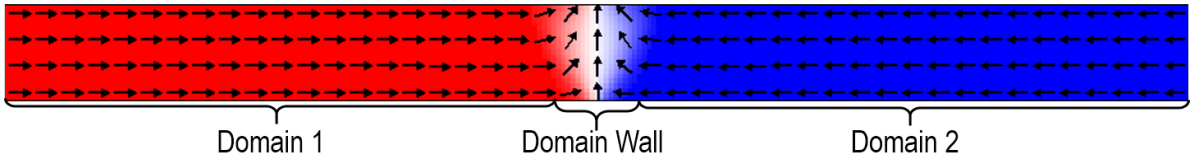


Figure 4.3: STT-driven Domain Wall motion.

For reading operations, a unidirectional current is applied to the Magnetic Tunnel Junction (MTJ) to sense the device state based on the Tunnel Magneto-Resistance (TMR) between MTJs fixed and free layers [99].

DWNM could be utilized as a logic gate, in which the states of the gate depend on the position of the DW in nanowire and is sensed using MTJ. The output of the gate is obtained based on the

[1]©2016 IEEE. Reprinted, with permission, from [96].

parallel (P) or antiparallel (AP) magnetization configuration of the MTJ fixed layer and DWNM nanowire, as shown in Figure 4.4(b).

Some recent surveys discussing the feasibility of integrating DWNM with CMOS address the interaction between their circuit design and manufacturing aspects [11, 100].

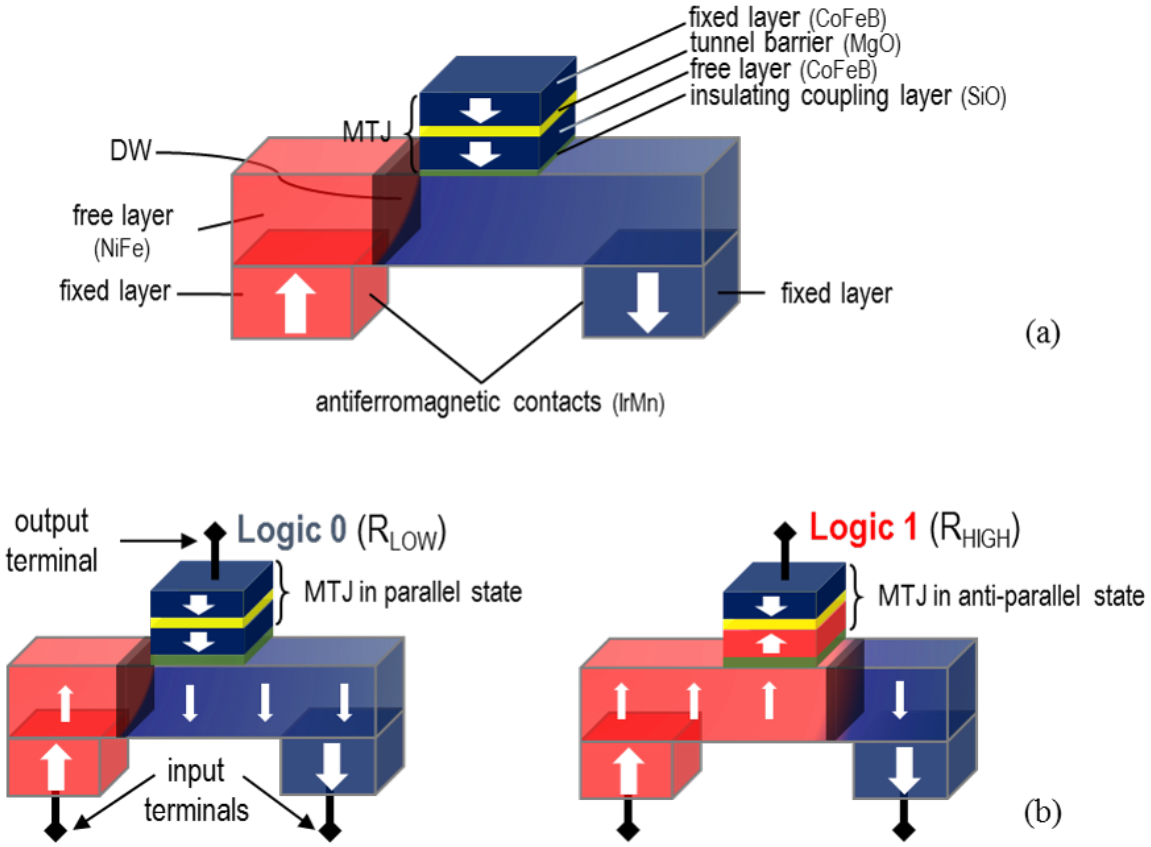


Figure 4.4: (a) Schematic illustration of DWNM device, (b) construction of a DWNM logic gate suitable for Boolean logic implementation.

For instance, the DWNM cell and cross-section view of its magnetic layers are shown in Figure 4.5, which depicts the DWNM integration at the back-end process of CMOS fabrication. Read and write operations are controlled by the Read/Write Word Lines connected to the gates of the access

transistors, which share a common Bit Line. Read access transistor is connected to MTJ that is integrated between the second and third metal layers. The nanowire is built in the third metal layer and controlled by Source Line, Bit Line, and the write access transistor, as shown in Figure 4.5(b).

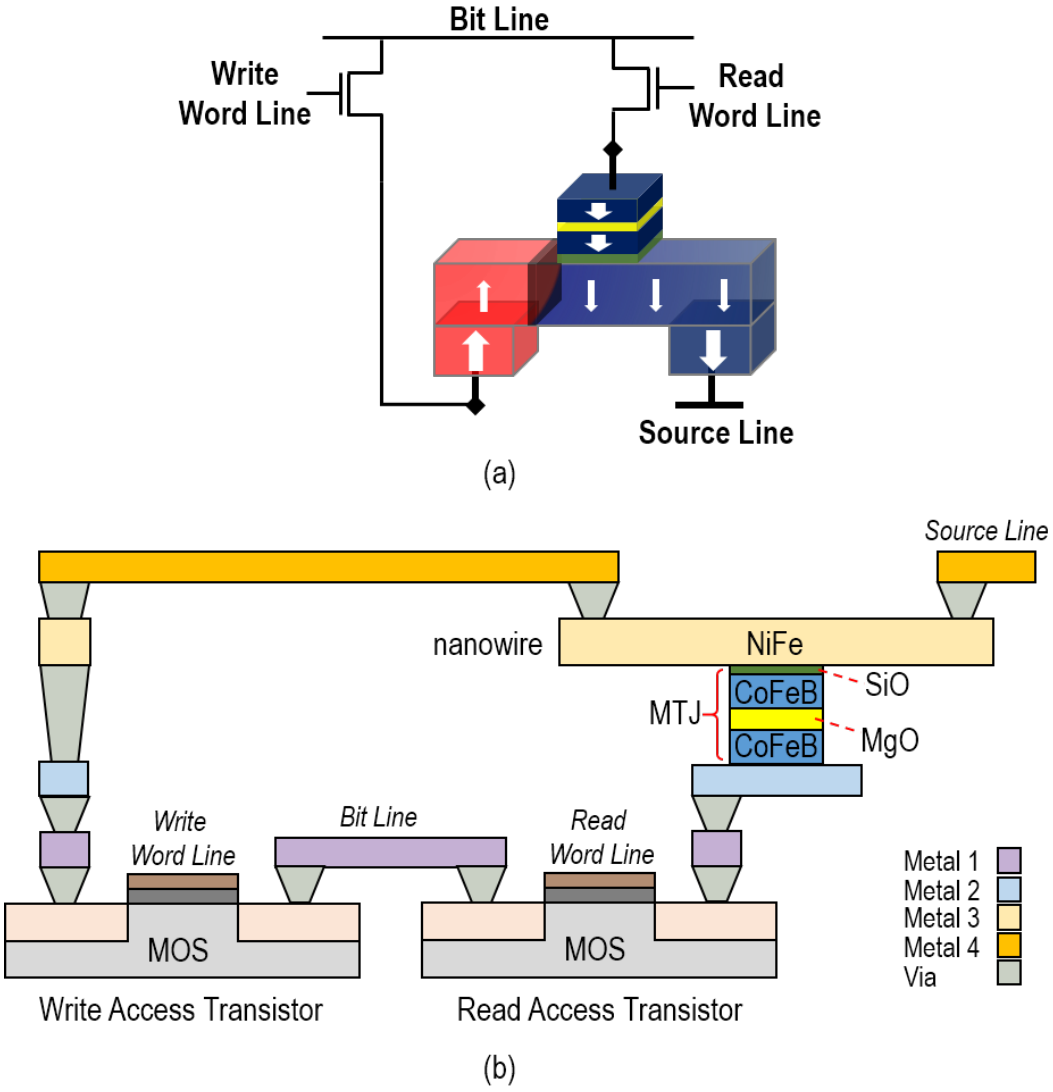


Figure 4.5: DWNM (a) cell design, and (b) cross sectional view.

Figure 4.6 shows the 1-bit DWNM-FA circuit consists of two DWNMs, two Sense Amplifiers (SAs), a CMOS inverter, and a Voltage Controlled Current Source (VCCS) [101].

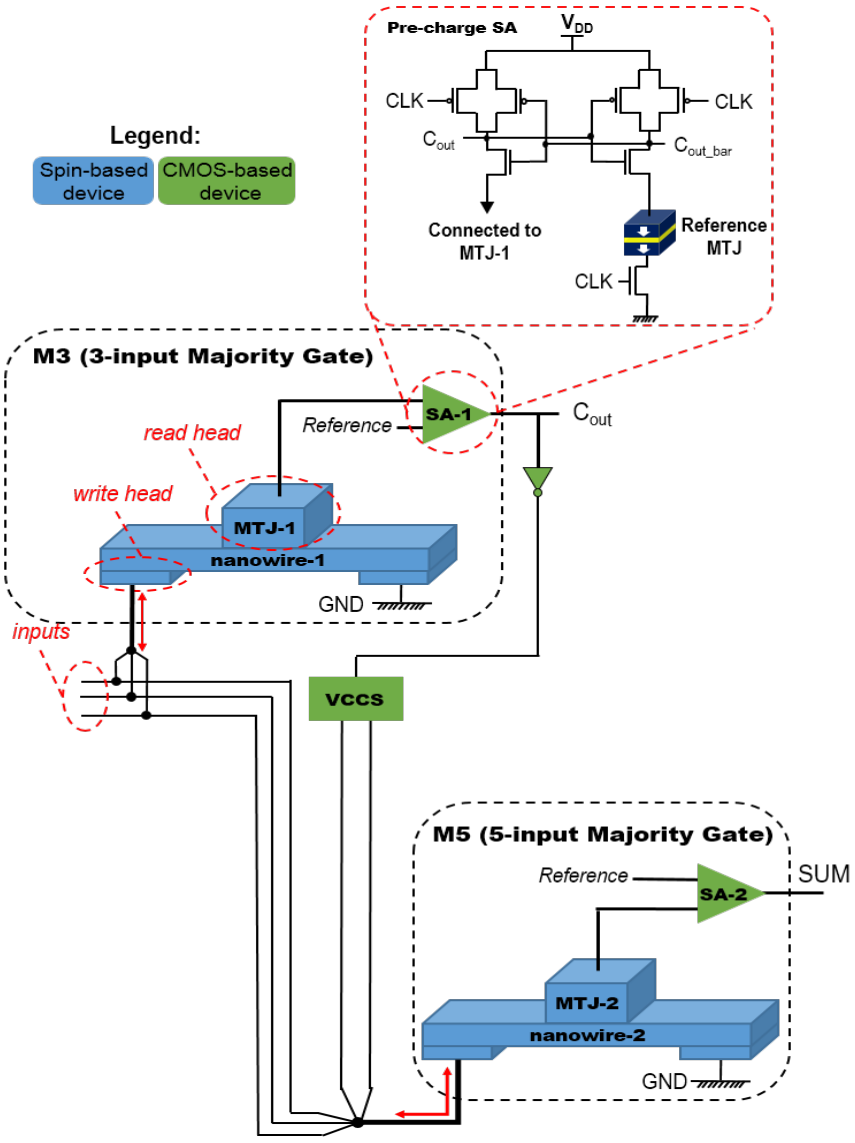


Figure 4.6: Schematic of DWNM based Full-Adder Circuit. The main structure is comprised of two DWNMs and two SAs, which operate as the functional building blocks and the decision-making elements, respectively.

The functionality of the circuit could be described as follows:

1) The inputs of the proposed circuit are bidirectional currents. Each of the three input currents is injected into the left terminal of M3, while its right terminal is connected to ground (GND), as shown in Figure 4.6. According to the conservation of current, the magnitude and direction of resultant current depend on the algebraic sum of the input currents. The resultant current moves the domain wall along the nanowire to realize a three-input MG.

2) Magnetization orientation of the MTJ-1 free layer is changed according to the nanowire-1 magnetic orientation determined by the position of the DW. Herein, pre-charge SAs are leveraged to sense the P or AP states of the MTJs [47, 102]. SA sensing process has two phases called pre-charge, and discharge. First, in the pre-charge phase, both SA branches are charged to V_{DD}. Then, the branches are isolated from V_{DD} and connected to GND in order to start the discharge phase. Each branch will discharge at a different speed based on its resistance. The side with lower resistance discharges faster and eventually outputs a "0" logic level, and vice versa. The reference MTJ resistance is designed in a manner such that its value in the parallel configuration is between low resistance (R_P) and high resistance (R_{AP}) of the MTJ cells, i.e. MTJ-1/MTJ-2, to properly sense its state. Reference MTJ cell and MTJ-1/MTJ-2 cell dimensions are listed in Table I. Figure 4.6 indicates that SA-1 outputs the state of nanowire-1, i.e. C_{OUT}.

3)C_{OUT} voltage is first inverted and then converted to current by means of a VCCS to be employed along with the primary three inputs of the circuit as inputs of the 5-input MG, which is built by nanowire-2 as depicted in Figure 4.6.

4) SA-2 outputs the state of the nanowire-2 which is the output of the FA circuit, at the terminal labeled SUM.

In the proposed circuit, we assumed logic "1" is equal to +200μA and logic "0" is -200μA. This

assumption is compatible with the required current mode operation since the sum of the input currents produces a bidirectional induced current which drives the DW to the left or right side of the nanowire based on the current direction. It also significantly reduces the routing complexity and peripheral circuits realizing the logic level corresponding to the position of the DW inside the nanowire.

In order to verify the functionality of our proposed circuit, SPICE circuit simulator with the parameters mentioned in Table 4.2 is utilized. The simulation includes the threshold current density which is required to unpin DW from its fixed position near the antiferromagnetic contacts. However, the stochastic behavior of the DWM device which is affected by the thermal fluctuations and edge roughness is not embraced. The 1-bit DWNM-FA simulation results along with the input and output waveforms are shown in Figure 4.7. All transitions matched the desired behavior while considering the propagation delays.

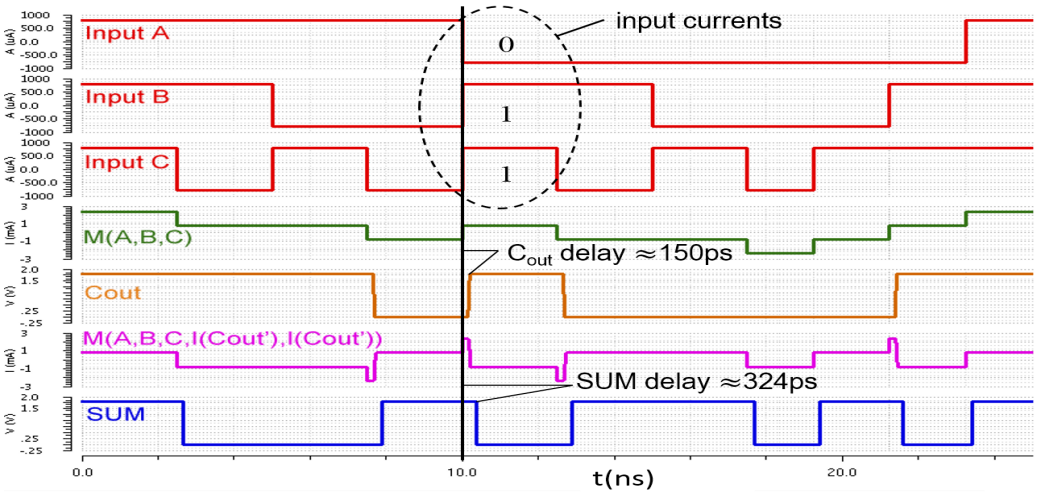


Figure 4.7: Simulation results of 1-bit DWNM based FA. Logic 0/1 levels of inputs (A, B, and C) correspond to applied currents of -200A and +200A whereas bits 0 and 1 for outputs, Cout and SUM, correspond to the voltage of 0V and 1.8V. For instance, input current pulses ABC=011 nucleate the DW in nanowire-1, Cout=1, and cannot unpin the DW in nanowire-2, SUM=0.

Table 4.2: Simulation Parameters of DWNM and MTJs.

Parameter	**Description**	**Value**
	$DW_{Length} \times DW_{Width} \times DW_{Thickness}$	100×10×3 nm^3
Area	MTJ-1/MTJ-2 Surface	100×65×$\pi/4$ nm^2
	Reference MTJ Surface	100×45×$\pi/4$ nm^3
t_{ox}	Thickness of oxide barrier	0.85 nm
α	Gilbert Damping factor	0.007
t_{free}	Thickness of free layer	1.3 nm
μ_B	Bohr Magneton	9.27 e-24 $J.T^{-1}$
P	Polarization (DWNM, MTJ)	0.75, 0.5
M_s	Saturation magnetization	200 8e5 $A.m^{-1}$
I_{C0}	Threshold Current Density	e10e12 A.m^-2
R_{AP}, R_P	MTJ-1/MTJ-2 Resistance	2.5 KΩ, 1.25 KΩ
R_p	Reference MTJ Resistance	1.8 KΩ
TMR	TMR ratio	100%
H_k	Out of Plane Anisotropy Field	1600∼1800 Oe
k_u	Uniaxial Anisotropy	400e3 J/m^3

Delay of the proposed Full-Adder circuit, t_{Cout} and t_{SUM}, is calculated using 4.6:

$$\begin{aligned} t_{Cout} &= t_{nanowire1} + t_{SA1} \\ t_{SUM} &= t_{Cout} + t_{inv-vccs} + t_{nanowire2} + t_{SA2} \end{aligned} \tag{4.6}$$

where $t_{nanowire1}$, $t_{nanowire2}$, t_{SA1}, and t_{SA2} are the nanowire-1, nanowire-2, SA-1, and SA-2 delays, respectively, and $t_{inv-vccs}$ is the delay of the inverter and VCCS together. Herein, $t_{nanowire1}$ and $t_{nanowire2}$ values are calculated using 4.7 and parameters mentioned in Table 4.2 as given by:

$$t_{nanowire1} = \frac{DW_{Length}}{u} \tag{4.7}$$

where u is the DW velocity which could be calculated using $u = \frac{\mu_B JP}{eM_s}$, and DW_{Length} is the length of the nanowire which is equal to 100nm in our design.

Table 4.3: Nanowire-1(for Cout) and Nanowire-2 (for SUM) Switching Delays.

A (μA)	B (μA)	C (μA)	$\sum inputs$	C_{out} (V)	$I(\overline{C_{out}})$ (μA)	nanowire-1 delay (ps)	$\sum inputs+$ $2\times I(\overline{C_{out}})$	SUM (V)	nanowire-2 delay (ps)
-800	-800	-800	-2.4 mA	0	+800	34.34	-800	0	103
-800	-800	+800	-800 μA	0	+800	103	+800	1.8	103
-800	+800	-800	-800 μA	0	+800	103	+800	1.8	103
-800	+800	+800	+800 μA	1.8	-800	103	-800	0	103
+800	-800	-800	-800 μA	0	+800	103	+800	1.8	103
+800	-800	+800	+800 μA	1.8	-800	103	-800	0	103
+800	+800	-800	+800 μA	1.8	-800	103	-800	0	103
+800	+800	+800	+2.4 mA	1.8	-800	34.34	+800	1.8	103
						Average $\approx$ 85.5			Average $= 103$

Nanowire delay is different for each set of inputs, due to the difference in input current. Table 4.3 provides the values for the nanowire-1 and nanowire-2 delays for each set of inputs. As listed in the Table, the average delay of nanowire-1 is roughly 85.8ps which is five sixths of a nanowire switching delay with single input current. Using a similar approach for calculating the delay of the nanowire-2 results in an average delay of 103ps which is equal to the delay of a single input nanowire.

Moreover, $t_{inv-vccs}$, t_{SA1}, and t_{SA2} are extracted using SPICE simulation in the 90nm technology library available and are equal to 23ps, 47ps, and 47ps, respectively. The nanowire delay has an inverse relation with the input current, as described in 4.8, where I is the input current.

$$t_{nanowire} = \frac{DW_{Length} \times eM_s}{\mu_B JP} = \frac{DW_{Length} \times eM_s \times DW_{Width} \times DW_{Thickness}}{\mu_B PI} \tag{4.8}$$

Equations 4.9 indicate that the FA circuit average delay, as calculated by 4.6 and 4.8 using the values obtained through SPICE simulation. The relation between the average delays of a DWNM-

FA circuit and input current are depicted in Figure 4.8.

$$
\begin{aligned}
t_{Avg-Cout} &= t_{Avg-nanowire1} + t_{SA1} = (\frac{5}{6})t_{nanowire} + 47(ps) \\
t_{Avg-SUM} &= t_{Avg-Cout} + t_{inv-vccs} + t_{Avg-nanowire2} + t_{SA2} = (\frac{11}{6})t_{nanowire} + 117(ps)
\end{aligned}
\tag{4.9}
$$

FA operation speed could be directly controlled by the value of the input currents, which could result in a high-speed arithmetic unit. However, this approach may not necessarily be power efficient. As previously mentioned, DWNM-FA circuit comprises two DWNMs, two SAs, a CMOS inverter, and a VCCS. Hence, the average power consumption of the proposed circuit, $P_{DWNM-FA}$, could be extracted using Equation 4.10.

$$
P_{DWNM-FA} = P_{Avg-nanowire1} + P_{Avg-nanowire2} + 2 \times P_{SA} + P_{inv-vccs} \tag{4.10}
$$

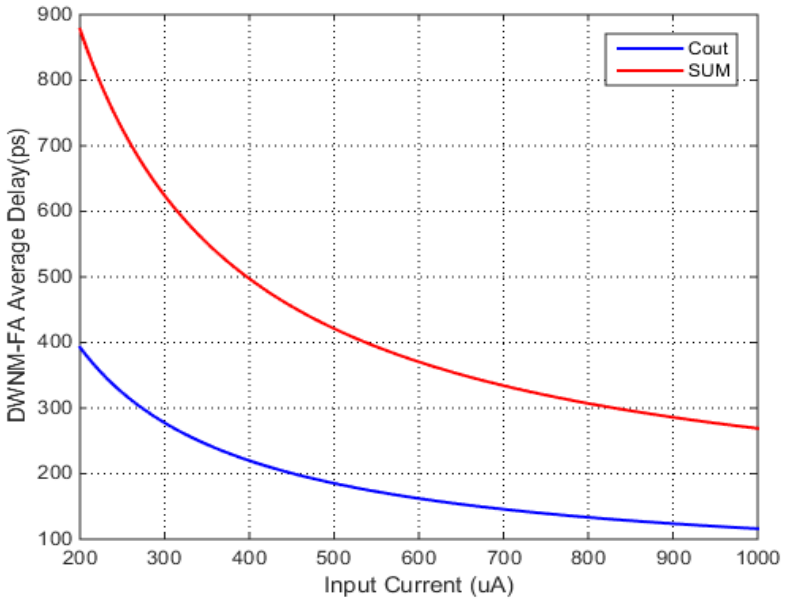


Figure 4.8: Dependence of DWNM-FA Average Delay on Input Current are depicted for circuit outputs Cout and SUM.

Herein, the demonstrated nanowire consumed power, Pnanowire, is expressed as below [103]:

$$P_{nanowire}(I,T) = R_0\big(1+\theta(T-T_0)\big)\times I^2$$
$$\text{where, } R_0 = \frac{\rho \times DW_{Length}}{DW_{Width}\times DW_{Thickness}} \tag{4.11}$$

where, T_0 is room temperature, i.e. 298K, R_0 is the resistance at T_0, temperature coefficient θ is considered +3e-3 K^{-1} at T_0, and ρ is the nanowire resistivity, which is considered 100 Γnm.

In a manner similar to that used to obtain the results listed in Table 4.3, the power consumption also varies based on different sets of inputs. Thus, a similar approach is employed for computing the average nanowire power consumption. At room temperature, the average power consumption obtained is $P_{Avg-nanowire1}$= $3P_{nanowire}$ = 640 μW and Pavg-nanowire2= Pnanowire=213.33 W. Furthermore, SA average power consumption, P_{SA}, and inverter and VCCS average power consumption, $P_{inv-vccs}$, are obtained respectively to be 13.6646 μW and 4.4277 μW by SPICE simulation in 90nm technology in the circuit delay time window. Finally, the relation between proposed DWNM-FA average power consumption, and input currents along with the temperature are extracted using 4.10 in conjunction with the values gained by SPICE simulation. Figure 4.9 exhibits a quadratic and linear growth for power consumption relative to the input current and temperature, respectively.

Finally, the Power-Delay Product (PDP) of the proposed DWNM-FA according to different values for input current and temperature are extracted utilizing 1.8V nominal voltage (V_{DD}) and 1 GHz circuit clock (CLK) frequency, as shown in Figure 4.10. The result illustrates a quadratic growth for PDP corresponding to the input current. As a result, based on the operating temperature of the proposed circuit and desired Power-Delay values, the optimum input current could be extracted from Figure 4.9 and Figure 4.10. Both iso-power and temperature constrained operating points can be readily obtained by the abovementioned surface plots.

Our designed tunable majority gate based FA can function in two different modes. 1) *Low Power Mode (LPM)*: the lowest current magnitude is injected, e.g. 200μA, as the input current, resulting in low power and low-speed operation of the FA circuit. 2) *High-Speed Mode (HSM)*: the highest magnitude current is injected as an input, e.g. 1 mA, so that the HSM FA design functions rapidly but with high power consumption. Comparison results with previous CMOS and MTJ based FAs fabricated using 180 nm CMOS process are summarized in Table 4.4. It shows that our design has a significant improvement in terms of area and complexity, i.e. device count. Moreover, MTJs are 2-terminal devices which share a common path for reading and writing operations that results in major reliability issues in MTJ-based designs [104, 105].

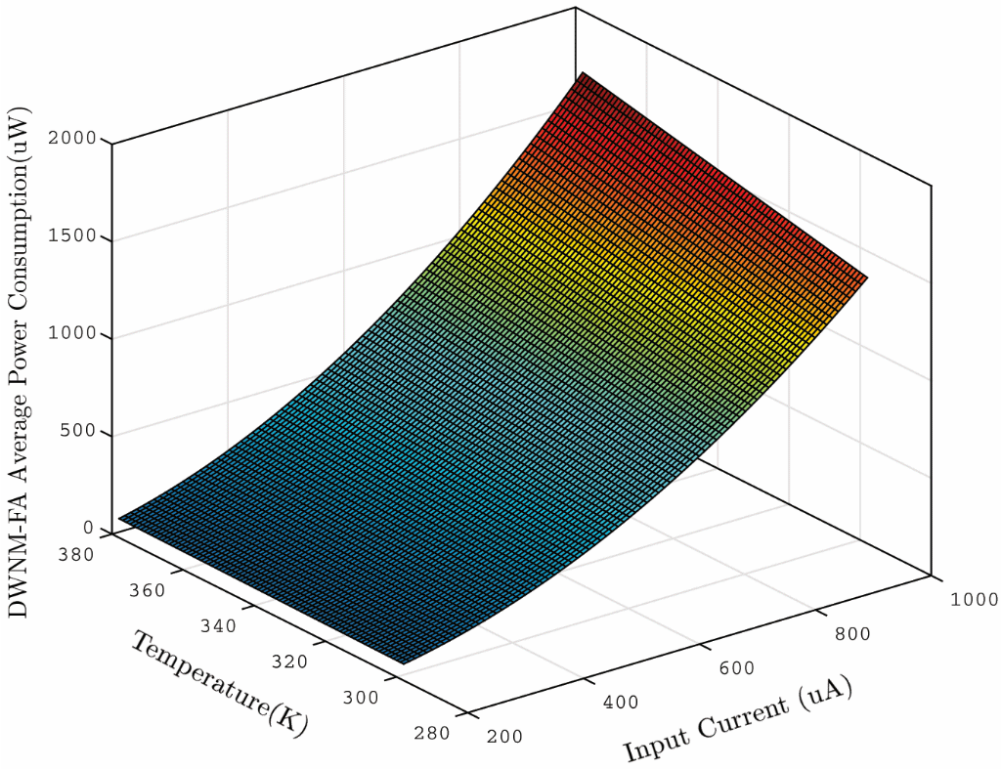


Figure 4.9: Power Consumption of DWNM-FA versus temperature and applied current.

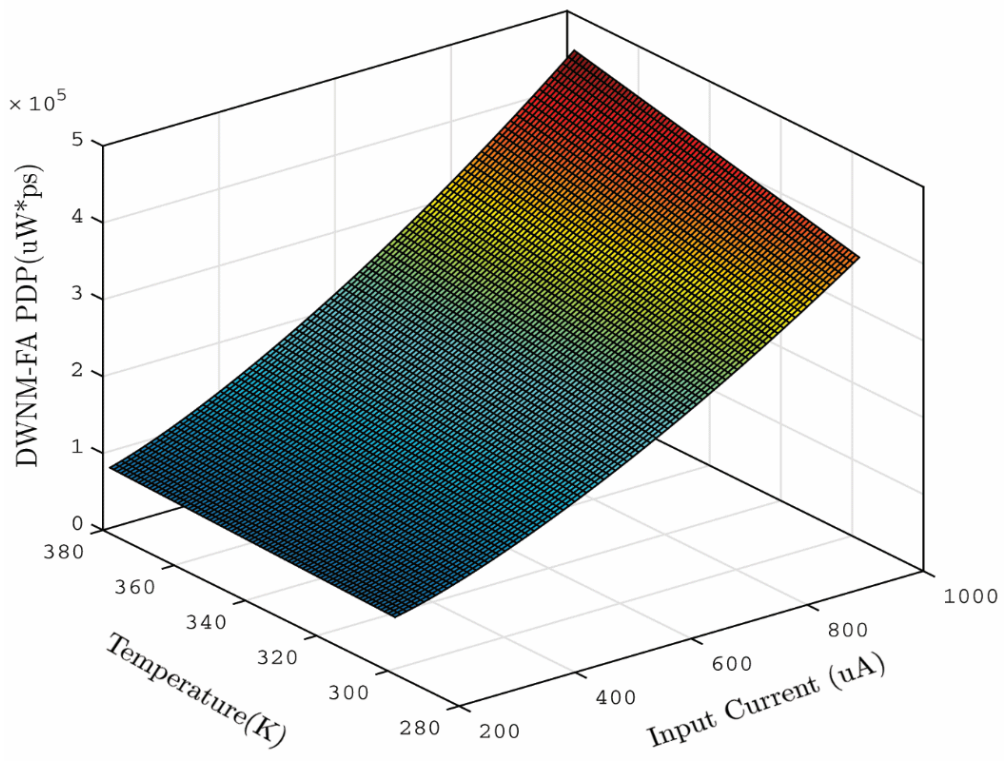


Figure 4.10: PDP of DWNM-FA versus temperature and applied current.

Whereas the DWNM employed in our design is a 3-terminal device enabling separate read and write paths that significantly reduce the disturbances induced by using a common path.

Table 4.4: Comparison of 1-bit Full Adders.

Parameter \ **Design**	CMOS [106]*	MTJ-based [106]	LPM [96]	HSM [96]
Delay	224 ps	219 ps	877 ps	269 ps
Dynamic Power (@1 GHz)	143 μW	33 μW	85 μW	1364 μW
Static Power	0.9 nW	0.0 nW	0.0 nW	0.0 nW
Area	333 μm^2	315μm^2	160 μm^2	
Complexity	42 MOSs	4 MOSs + 4 MTJs	20 MOSs + 4 MTJs + 2 nanowires	

*Full Adders are fabricated using 180 nm CMOS process

Based on the obtained result from the previous design and STT switching drawbacks, we have designed a non-volatile FA using SHE-MTJ devices. Our proposed FA is composed of 23 MOS transistors and three SHE-MTJs. Two of the SHE-MTJs function as majority gates (MGs), and the other one is utilized as a reference element to sense the output of the FA. The switching behavior and functionality of the proposed circuit are verified using SPICE circuit simulator. Figure 4.11 depicts the schematic of our proposed FA, which consists of two main parts as described below[2].

Write/Reset Circuit: for SHE-MTJ write operation, a charge current should be applied to the HM to produce a spin current greater than the critical switching spin current of the MTJ. In our SHE-based FA design, three PMOS transistors are leveraged to produce the input charge current according to the three inputs of the circuit, A, B, and C_{in}. The magnitude of the driven current for SHE-1 is determined based on the conservation of current on the N1 node shown in Figure 4.11.

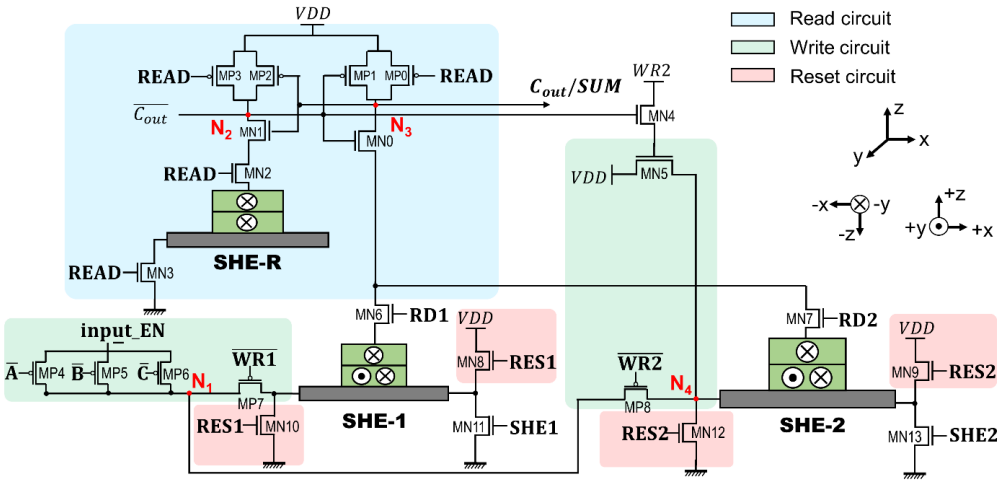


Figure 4.11: Circuit-view of SHE-based FA design. SHE-1 functions as a 3-input MG, while SHE-2 performs 5-input MG function.

[2]©2017 IEEE. Reprinted, with permission, from [107]

The dimensions of the SHE-1 is designed in a manner such that its switching critical current is higher than a charge current produced by one of the input PMOS transistor (MP_4, MP_5, and MP_6). In order for the C_{out} to become "1", the SHE-1 state should change to anti-parallel. Hence, at least two of the three input transistors are required to be ON to switch the SHE-1 state. Therefore, the three PMOS transistors and SHE-1 device together function as a 3-input MG. To perform the SHE-1 write operation, RES1, WR1, and SHE1 signals should be "0", "1" and "1", respectively. For reset operation, two NMOS transistors (MN_8 and MN_{10}) are assigned to reset the SHE-1 state and prepare it for the next operation. Herein, reset operation means writing on SHE-MTJs in the -x direction to change their configuration to P state.

To implement the 5-input MG required for producing the SUM output, $\overline{C_{out}}$ is obtained through a sense amplifier, and MN_5 transistor is used to produce a current based on the obtained $\overline{C_{out}}$. The size of the MN_5 transistor is designed in a manner such that it generates a current amplitude approximately twice as large as the currents produced by input PMOS transistors (MP_4, MP_5, and MP_6). Therefore, it can be assumed that there are five input currents injected to SHE-2.

The magnitude of the current applied to the HM of the SHE-2 is determined based on the conservation of the aforementioned currents in N_1 node. Dimensions of the SHE-2 is designed in a way that at least three out of the five inputs should be applied to HM to produce a current amplitude greater than the critical current of SHE-2. Thus, SHE-2 functions as a 5-input MG. SHE-1 read operation and SHE-2 write operation should be performed simultaneously. Therefore, all of the RD1, SHE1, WR2, and SHE-2 signals should be "1" during this operation. The reset mechanism for SHE-2 is similar to that of the SHE-1. However, it can be improved by performing the reset operation only when Cout equals "1". Thus, unnecessary reset operations will be removed, which can decrease the energy and delay overhead caused by the reset scheme. The dimensions of the SHE-MTJs used herein are listed in Table 4.5.

Table 4.5: Simulation Parameters of SHE-based FA.

Parameter	Description	Value
SHE-R	HM Volume (L×W×T)	120×60×3 nm^3
	MTJ Area (L×W)	60×30×$\pi/4$ nm^2
SHE-1	HM Volume (L×W×T)	100×60×3 nm^3
	MTJ Area (L×W)	60×30×$\pi/4$ nm^2
SHE-2	HM Volume (L×W×T)	150×80×3 nm^3
	MTJ Area (L×W)	80×40×$\pi/4$ nm^2
θ_{SHE}	Spin Hall Angle	0.3
ρ_{HM}	Resistivity	200 $\mu\Omega.cm$
ϕ	Potential Barrier Height	0.4 V
t_{ox}	Thickness of oxide barrier	1.2 nm
α	Gilbert Damping factor	0.007
M_s	Saturation magnetization	200 7.8e5 A.m^{-1}

The SHE-MTJs are designed in a specific dimension to match with circuit requirements for providing optimal sensing performance with one reference (SHE-R).

Read Circuit: The main component of the reading scheme is a pre-charge sense amplifier. To perform proper sensing operation, the reference SHE-MTJ device (SHER) is designed in a way that its resistance value in the parallel configuration is between low resistances (R_{P_S}) and high resistances (R_{AP_S}) of the SHE-1 and SHE-2 cells. Table 4.6 elaborates the required signaling for performing the write, read, and reset operations.

To verify the functionality of proposed SHE-based FA design, SPICE circuit simulator and SHE-MTJ model with parameters mentioned in Table 4.5 are utilized. Figure 4.12 shows the functionality of our proposed SHE-based FA, in which the applied inputs are ABC="010".

Write, read, and reset operations are indicated by green, blue, and red colored shading, respectively. There are three phases for one complete operation cycle of SHE-FA. In phase I, shown in Figure 4.12 (a), write and reset transistors for SHE-1 and SHE-2 are enabled, respectively. The produced input charge current according to ABC= "010" equals 94 μA, which is smaller than SHE-1 critical

Table 4.6: Required signaling for 1-bit SHE-based FA.

Operation	Device	Signaling
WRITE	SHE-1	READ= "0", WR1= SHE1= "1"
	SHE-2	WR2= SHE2= SHE1= RD1= READ= "1"
READ*	SHE-1	RD1= SHE1= READ = "1"
	SHE-2	RD2= SHE1= READ= "1"
	SHE-R	READ= "1"
RESET	SHE-1	RES1= "1"
	SHE-2	RES2= "1"

$(*)$ When READ is set("1"), node N_2 in Fig. 3 is connected to the ground via SHE-R, which is in a parallel configuration.
$R_{SHE\text{-}1\ (P)}, R_{SHE\text{-}2\ (P)} < R_{SHE\text{-}R\ (P)} < R_{SHE\text{-}1\ (AP)}, R_{SHE\text{-}2\ (AP)}$

current, i.e. $I_{C\text{-}SHE1}$=108 μA. Thus, the FL magnetization direction of SHE-1 remains in P state. Simultaneously, the SHE-2 reset transistors generate a 164 μA current amplitude in x-direction, which can reset SHE-2 to P state in 2.07ns.

Figure 4.12 (b) depicts the second phase of SHE-FA operation including reading SHE-1 and writing SHE-2 devices at the same time. As mentioned above, since the SHE-1 input current for ABC= 010 is not sufficient to switch its states, C_{out} and $\overline{C_{out}}$ equal "0" and "1", respectively. Therefore, MN4 and MN5 transistors are ON, and $I_{\overline{C_{out}}}$ will be generated. Input currents and $I_{\overline{C_{out}}}$ are accumulated in N4 node, and produce the SHE-2 write current. In this example, the magnitude of the injected current equals 146 μA, which is greater than SHE-2 critical current, i.e. $I_{C\text{-}SHE2}$=139 μA. Thus, the state of the SHE-2 device changes to AP configuration.

In the third phase, the reset and read operations are performed for SHE-1 and SHE-2, respectively. Due to the difference between the resistances of the SHE-1 and SHE-2 HMs, the produced reset current for SHE-1 is different from that of the SHE-2. SHE-1 reset current equals 170 μA, which result in a 1.73 ns delay for the SHE-1 reset operation. In this phase, SHE1 and SHE2 signals are equal to "0" and "1", respectively. Thus during the read operation, PCSA senses the state of the

SHE-2 device that is the SUM output. As mentioned above, SHE-2 was configured to AP state in the second phase, therefore the output of the PCSA equals "1". Simulation results including timing diagram and SHE-MTJs' magnetization directions are depicted in Figure 4.13, which validates the functionality of our proposed FA for two sets of inputs, ABC= "001" and ABC= "111". Propagation delays, produced charge currents, and power consumption for all possible input combinations are listed in Table 4.7. Table 4.8 provides a comparison between our 1-bit SHE-based FA and previous CMOS-based and MTJ-based 1-bit FAs [106] in terms of delay, area, power consumption, and complexity. The current-mode FAs that are proposed in [96, 108] are excluded from our comparison. Herein, we have examined the functionality of an n-bit SHE-FA to verify the concatenatability of our SHE-based FA. Figure 4.14 shows the schematic and timing diagram for a 4-bit SHE-FA.

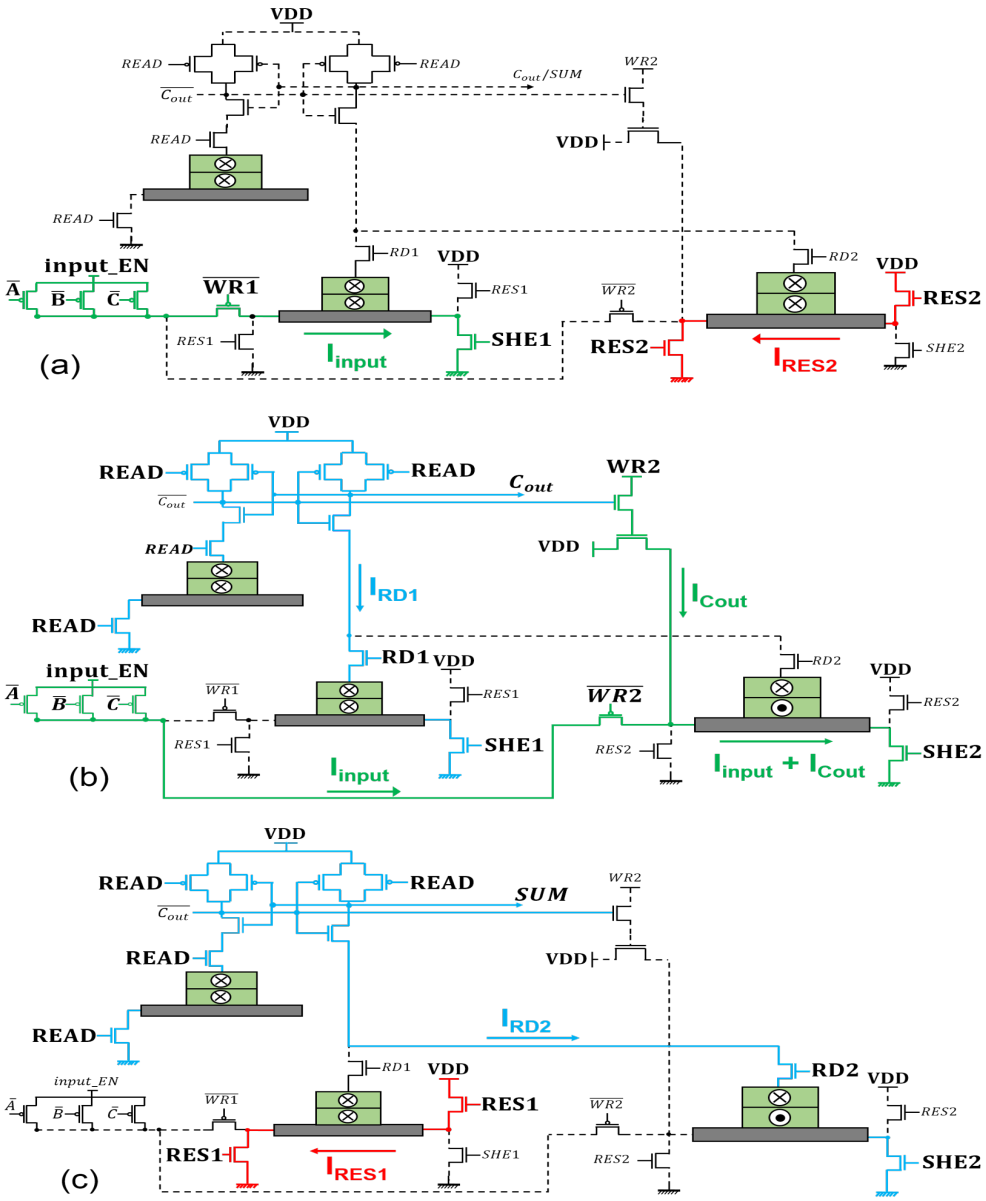


Figure 4.12: SHE-based functionality for input ABC = "010" (a) write and reset operations for SHE-1 and SHE-2 occurred, respectively, I_{input} = 94 μA < $I_{C\text{-}SHE1}$; hence, FL of SHE-1 remains in P state, then (b) read and write operation for SHE-1 and SHE-2 perform simultaneously, in which injected current through SHE-2 is 146 μA > $I_{C\text{-}SHE2}$, so FL of SHE-2 changes to AP state, and finally (c) SHE-1 is reset along with reading SHE-2 state.

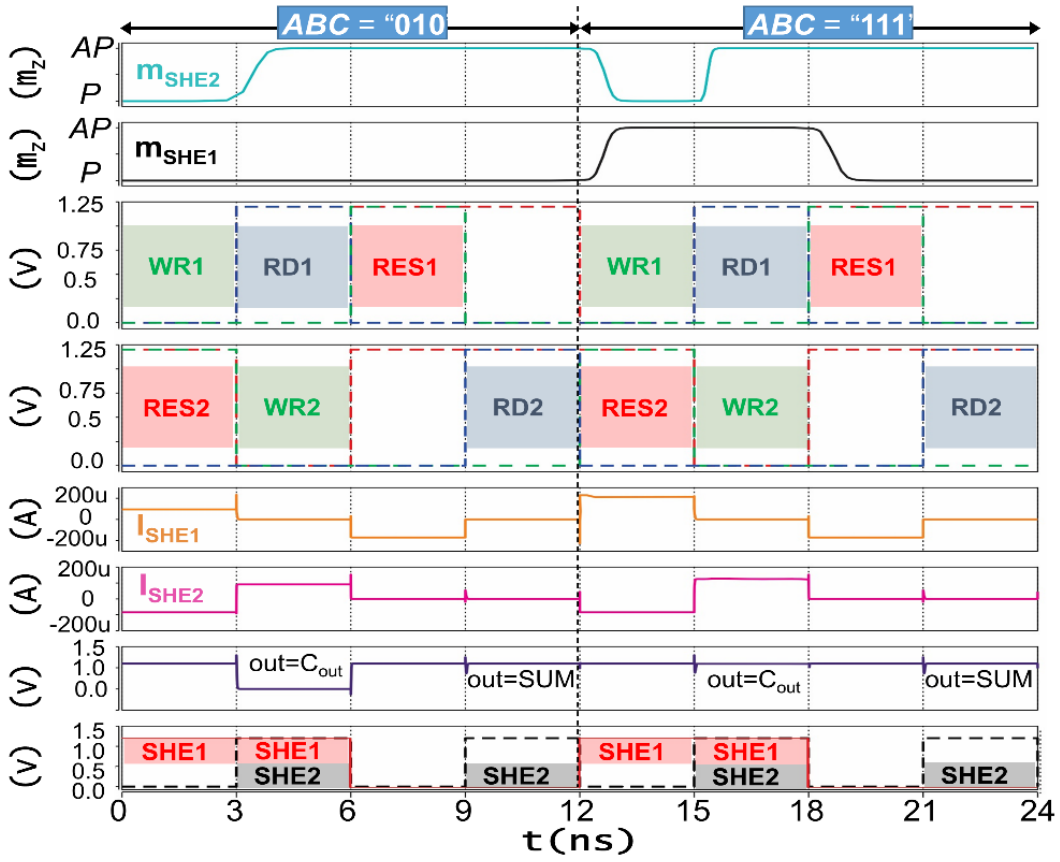


Figure 4.13: Simulation results of 1-bit SHE-based FA for two input sequences, "010" and "111".

Table 4.7: SHE-based FA Performances for all Input Combinations.

Standard functions			$\mathbf{I_{SHE1}}$	**Power** (μW)		**Delay**		$\mathbf{C_{out}}$	$\mathbf{I_{SHE2}}$	**Power** (μW)		**Delay**		**SUM**
A	B	C	(μA)	**write**	**read**	**write**	**delay**		(μA)	**write**	**read**	**write**	**read**	
0	0	0	0	0	14.72	N/A	41 ps	0	112	137	14.72	N/A	41 ps	0
0	0	1	94	113	14.72	N/A	41 ps	0	146	178	12.4	2.7 ns	30 ps	1
0	1	0	94	113	14.72	N/A	41 ps	0	146	178	12.4	2.7 ns	30 ps	1
0	1	1	136	162	12.4	2.25 ns	30 ps	1	135	163	14.72	N/A	41 ps	0
1	0	0	94	113	14.72	N/A	41 ps	0	146	178	12.4	2.7 ns	30 ps	1
1	0	1	136	162	12.4	2.25 ns	30 ps	1	135	163	14.72	N/A	41 ps	0
1	1	0	136	162	12.4	2.25 ns	30 ps	1	135	163	14.72	N/A	41 ps	0
1	1	1	136	188	12.4	1.89 ns	30 ps	1	157	189	12.4	2.45 ns	30 ps	1

Table 4.8: Comparison of logic-in-memory 1-bit full adder circuits.

Parameter	CMOS [106]	MTJ- based [106]	developed herein
Delay*	2.2 ns	10.2 ns	7 ns
Dynamic Power†	2 mW	2.1 mW	0.71 mW
Static Power	0.9 nW	0	0
Area	333 μm^2	315 μm^2	180 μm^2
Device Count	42 MOSs	34 MOSs + 4 MTJs	23 MOSs + 3 SHEs

($*$) Total delay including write and read operations.

($\dagger$) Dynamic power depends on the number of current paths from V_{DD} to GND, which is lower in spin-based designs compare to CMOS-only implementation.

To obtain the SUM output for each adder block, C_{out} of their previous block is required to be applied as one of the three input signals. Hence, each C_{out} bit in level n is utilized to obtain, (1) SUM output in level n, and (2) C_{out} bit in level n+1. Therefore, the C_{out} in each level should remain unchanged for a sufficient duration to ensure the correct operation of an n-bit SHE FA. This can be achieved by SHE-MTJ devices without any additional energy consumption, due to their non-volatility feature. The timing limitations are considered in the timing diagram shown in Figure 4.14. To decrease the propagation delay of an n-bit SHE-FA, the independent operations are designed to be performed simultaneously. Namely, C_{out} write operation for the second adder block is independent of the SUM write operation of the first block, thus both are operated in the second time step.

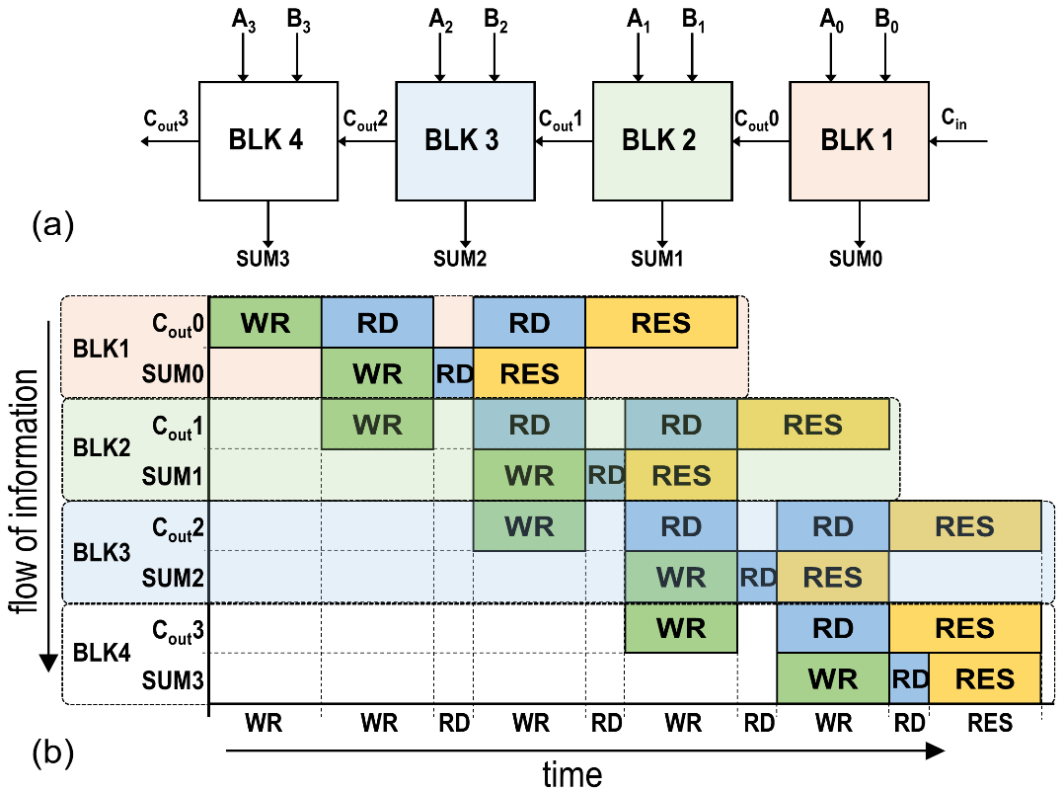


Figure 4.14: Schematic of 4-bit SHE-based FA and its timing diagram.

Power consumption of an n-bit SHE-FA relies on the number of write, read, and reset operations that are required to be executed for a complete addition cycle. For instance, there are 8 SHE-MTJs in a 4-bit SHEFA, thus eight write and reset operations should be performed in a complete addition operation. Moreover, as shown in Figure 4.14, eleven read operations are performed in a complete cycle; eight operations to output the SUM and C_{out} values and three operations for switching SHE-2 states.

In general, the total propagation delay and power consumption of our proposed n-bit SHE-based

FA can be calculated using below equations:

$$D_{\text{n-FA}} = DWR_{\text{SHE-1}} + N \times (DWR_{\text{SHE-2}}) + N \times (D_{SA}) + DRES_{\text{SHE-2}} \tag{4.12}$$

$$P_{\text{n-FA}} = 2N \times \left[\max(PWR_{\text{SHE-2}})\right] + 2N \times (PRES_{\text{SHE-1}}) + \big(2(N\text{-}1)+(N+1)\big) \times (PRD_{\text{SHE-1}}) \tag{4.13}$$

where, N is a number of bits, $DWR_{\text{SHE-1}}$ and $DWR_{\text{SHE-2}}$ are write operation delays of SHE-1 and SHE-2, respectively. DSA is PCSA delay, and $DRES_{\text{SHE-2}}$ is reset operation delay of SHE-2. $PWR_{\text{SHE-2}}$, $PRES_{\text{SHE-1}}$, and $PRD_{\text{SHE-1}}$ are the power consumption of SHE-2 write, SHE-1 reset, and SHE-1 read operations, which are the worst case values for each quantity.

Our SHE-based FA was examined using SPICE circuit simulator, which indicated 76% and 32% improvements in terms of energy consumption and area over the previous spin-based FA, respectively. Due to the scalability and voltage-based operation of our proposed 1-bit SHE-FA, it can be readily concatenated to constitute an n-bit SHE-based adder or an n-bit SHE-based ALU with the significantly low area and energy consumption as depicted by the pipeline analysis.

CHAPTER 5: SPIN-BASED NORMALLY-OFF COMPUTING APPROACHES

Scaling of MOS devices increases leakage power, becoming an increasingly significant part of the total energy consumption in a wide range of processor designs [109]. MOS scaling challenges have inspired considerable advancements in reduced-power datapath designs. Effective techniques to reduce dynamic energy consumption, such as low-voltage operation, clock gating, and efficient RTL design have been widely-successful [110, 111, 112]. Nonetheless, an increasing number of modern smart systems from many-core dies to Internet-of-Things (IoT) components may reside in various sleep modes for a significant proportion of their lifetime, making the standby power dissipation of such systems a critical issue, especially under the deep-scaling impacts of CMOS process technology.

For this reason, various state-of-the-art *Normally-off Computing (NoC)* techniques have been developed, which provides promising features such as zero standby power consumption during idle time, instant wake-up time, and resilience to power failure [113, 114, 115, 116]. Hence, nonvolatile elements including non-volatile memories (NVMs) and non-volatile flip-flops (NV-FFs) have received increasing attention because of their utility in designing an NoC architecture [117, 118]. The NV elements eliminate the otherwise-required boot-up step after sleeping, due to their non-volatility. Generally, in NV processors, data from all registers are stored in NV-FFs before going into a deep sleep mode. During sleep mode, no power source is needed. After powering up the chip, data from NV-FFs is restored and the system resumes its operation. Various hardware-assisted approaches for normally-off computing have recently been promulgated [109, 110]. For instance, in [119, 120], all of the conventional FFs are replaced by NV-FFs, while in [109], many small NV memory arrays are utilized to backup and restore data. Although NV elements offer the de-

sirable feature of non-volatility, their advantages are achieved at the cost of increased write-power consumption. Hence, a comprehensive datapath synthesis strategy is essential.

In previous approaches, the roles and costs of the additional middleware and checkpointing operations needed have been prominent [71, 74], as was discussed previously. In addition to the overheads resulting from the checkpointing operations themselves, existing approaches may suffer from leakage occurring between the checkpointing operations made to non-volatile backup storage. Namely, the registers and flip-flops within CMOS-only datapaths are volatile, which makes power-gating challenging [121].

Herein, we develop a new duty-cycle-variable computing approach to facilitate and invigorate energy-harvesting-powered Internet of Things (IoT) devices. The proposed *Elastic Intermittent Computation (EIC)* foundations are advanced from the ground up by extending emerging post-CMOS switching elements to realize polymorphic majority-gate logic that is intrinsically-capable of middleware-coherent, battery-free, intermittent computation without checkpointing, micro-tasking, or software bloat and energy overheads. The research is initiated with Spin Hall Effect SHE-MG and SHE-PG cell libraries. Then, a SHE-based Synthesis and Optimization Routine and Tool (SHE-SORT) is developed to implement Boolean gates and logic circuits based on the developed libraries. Finally, the NV-Clustering methodology is defined, which utilizes the optimized SHE-PG and SHE-MG libraries to develop non-volatile datapaths for intermittent-robust energy harvesting processing units.

NV FFs For Normally-Off Computing

To implement normally-off computing architectures using hardware-based approaches, NV-FFs fulfill essential roles. They are utilized within power-gated architectures [117, 118, 122] and within

intermittent computing systems [121, 107, 123], as overviewed in this Section[1].

NV-Assisted Power Gating

Several software/hardware based mechanisms for reducing standby or leakage energy consumption can directly benefit from the utilization of NV elements. One of the most widely-deployed methods is power gating, in which supply energy is selectively disabled for idle blocks of system on chip (SoC) resources via power gating signals. Whereas unprotected power gating results in data loss, it is necessary to consider data and state maintenance mechanisms, such as retention flip-flops to rapidly store/restore internal states [109]. Since retention flip-flops are always powered up, leakage power becomes a central challenge. Hence, the introduction of NV-FFs eliminates the need for alternatives to virtual VDD/ground grids. A schematic of NV-FFs depicting connections of the NV element to the volatile CMOS-based flip-flop is shown in Figure 5.1. This includes conventional CMOS master and slave latches and an NV latch, consisting of NVM as well as write and read circuitry. When a power gating signal is received, the flip-flop stores its state in NVM and subsequently becomes dis-connected from VDD/ground. Upon resumption of power, its contents are restored from NVM. There is extensive research designing NV-FFs using different NV elements such as STTMRAM (MTJ, SHE) [125, 126], PCRAM [127], ReRAM [128], and FeRAM [110]. In some of these, a conventional FF is connected to a write circuit to write the state to an NVM, which is connected to the read component [129].

Whereas, in several designs, a master latch is connected to a write driver in order to write into an NVM and a read circuit connected between the NVM and a slave latch. To reduce area overhead, read sensing schemes can be merged with the master or slave latch [130]. However, it results in two concerns: (1) low sensing cur-rent that reduces operating speed while increasing read disturbance

[1] ©2018 IEEE. Reprinted, with permission, from [123, 124]

probability, and (2) insufficient write current.

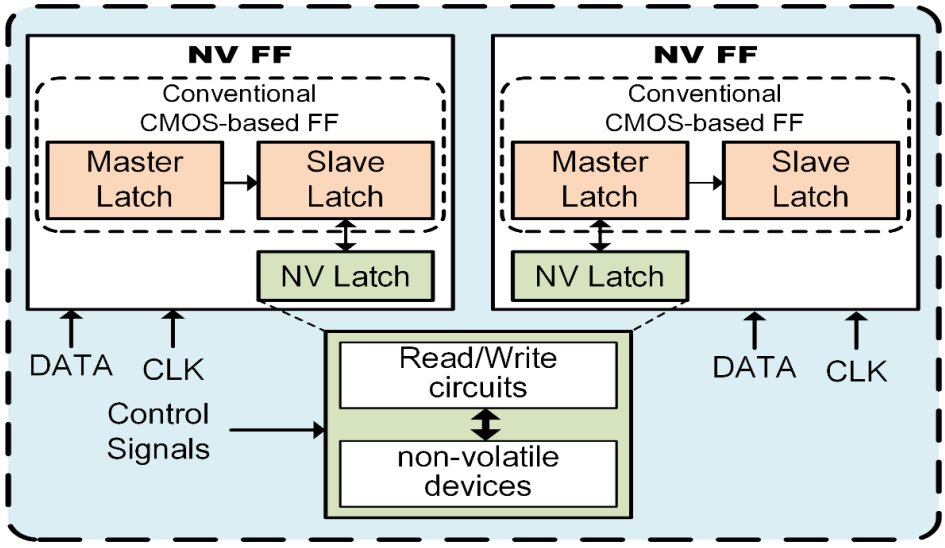


Figure 5.1: Block diagram of NV-FFs, (left) modified slave stage, and (right) modified master stage.

NV-Enabled Intermittent Computing

Another upcoming deployment of NV-FFs is within energy-harvesting systems. Energy-harvesting-powered computing offers intriguing and vast opportunities to dramatically transform the landscape of IoT devices [131] and wireless sensor networks [132]. These devices require greatly-reduced energy consumption, such that they can operate using only ambient sources of light, thermal, or kinetic [21] energy. On the other hand, intermittent behavior can result in disturbances in the execution of programs, data loss, glitch conditions, and lack of execution progress that may lead to irregular and unpredictable results [133]. Therefore, there are several software/hardware -based approaches proposed for tolerating intermittency. In most of them, a check-pointing approach is utilized to ensure the accurate forward progress of computation, whereby any volatile

execution context is proactively preserved in an NV-FF prior to anticipated periods of power failure. In [75] a software-based model for programming intermittent devices is presented, in which forward-progress is ensured at the task granularity level. It utilizes idempotent processing concepts to make tasks restartable. In addition to NV-FFs, these systems consist of voltage detection sensors including capacitor arrays to detect the power failure and also to provide backup energy after the occurrence of power failure. Meanwhile, critical states of the processor will be partially-retained. Figure 5.2 shows a block diagram of intermittent-robust systems using NV-FFs, which are evaluated herein via simulation using SPICE.

The abovementioned general checkpointing-based approach may suffer from internal and external inconsistencies after each power loss. Internal inconsistency occurs when the execution context is partially-retained in NVM, while external inconsistency arises when the power failure occurs between two checkpoints [134]. Moreover, ancillary circuits are needed, such as capacitor arrays and voltage detection systems, which impose large area overheads, which is a critical challenge for area-constrained IoT devices. On the other hand, conventional NV-FF/register based designs are not able to detect power failure, to store and to retain checkpoints without these additional circuits.

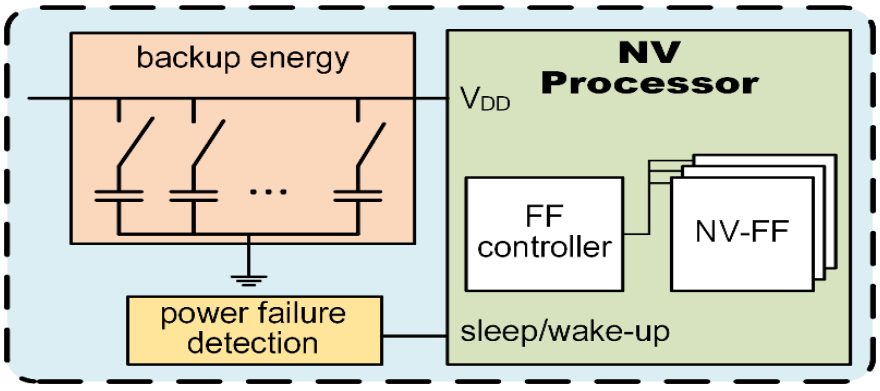


Figure 5.2: Overall structure of intermittent resilient architecture.

SHE-based Majority Gate Cell Library

Based on the previous discussions, the importance of MG and resemblance between MGs functionality and behavior of Spintronics, we develop SHE-based 3- and 5- input MG cell libraries by which MGs can be cascaded to realize conjunctive/disjunctive Boolean gate realizations. Figure 5.3 (a) and (b) show the schematic of 3-input and 5-input Majority Gates (MGs), respectively, which are designed using SHE-MTJ devices. Each cell consists of one SHE-MTJ and one PCSA, namely SHE-MG. Thanks to the PCSA structure, we have two complementary outputs, out and $\overline{\text{out}}$, which provides both *Majority* and *minority* functions. Since only universal gates can implement any Boolean functions alone, MG-based implementation requires inverters. Whereas, our SHE-MG cell can implement any Boolean function without the need to use any other gate type. The results related to reading and switching operations of 3- and 5- input SHE-MGs are illustrated in Tables 5.1 - 5.3. By affixing one (or two) of the three (or five) input transistors in ON or OFF states upon demand during the circuit operation, then a 2(or 3)-input OR gate or a 2(or 3)-input AND gate can be realized, respectively. For instance, the functionalities of 2-input OR and 3-input AND gates implemented by SHE-MTJ based MGs are validated by SPICE shown in Figure 5.3 (c). These results will be extended to spin-based Polymorphic Gates (PGs) that utilize intra-gate control to provide a functionally-complete set of Boolean logic expressions.

Table 5.1: Switching results for 3-input SHE-MG.

Inputs			**No.**†	**Write Operation**	
A	B	C		**Power (μW)**	**Delay (ns)**
0	0	0	1	0.124	-
0	0	1	3	67.7	-
0	1	1	3	130.3	2.98
1	1	1	1	187.9	1.91
Average				**97.7**	**2.84**

(†)Number of 3-input Boolean expression with the same features.

Table 5.2: Switching results for 5-input SHE-MG.

Inputs					No.†	Write Operation	
A	B	C	D	E		Power (μW)	Delay (ns)
0	0	0	0	0	1	0.32	-
0	0	0	0	1	5	67.2	-
0	0	0	1	1	10	128.4	-
0	0	1	1	1	10	185.4	2.22
0	1	1	1	1	5	236.64	1.69
1	1	1	1	1	1	283.68	1.39
Average						**154.4**	**2.11**

(†)Number of 5-input Boolean expression with the same features.

Table 5.3: Read operation results for 3- and 5- input SHE-MGs.

Design	Read "0"		Read "1"	
	Power	Delay	Power	Delay
SHE-based 3-MG	1.64 μW	20 ps	1.28 μW	20 ps
SHE-based 5-MG	1.35 μW	21 ps	1.53 μW	22 ps

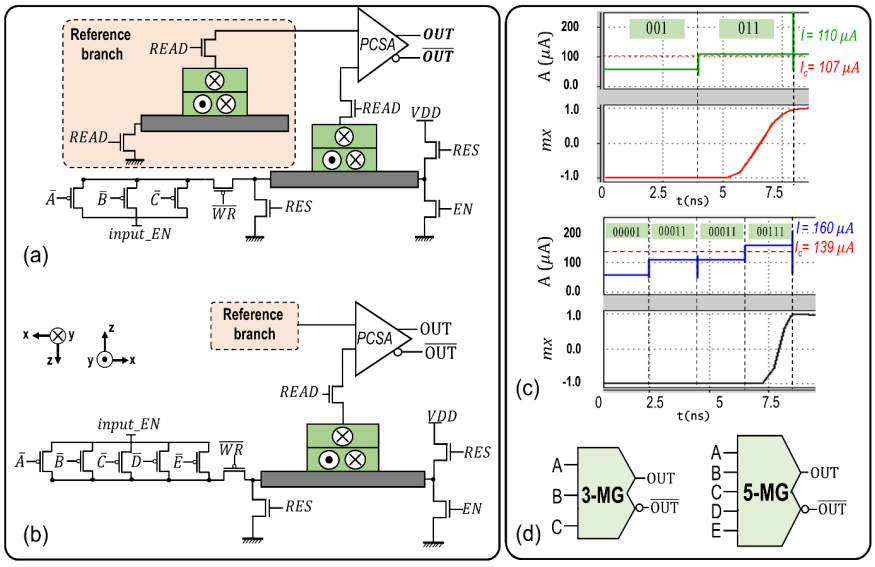


Figure 5.3: (a) SHE-MTJ based 3-input MG, (b) SHE-MTJ based 5-input MG. Simulation results for (c) 2-input OR logic, and 3-input AND logic using MG3 and MG5, respectively, (d) 3-input and 5-input SHE-MTJ based MGs.

Proposed SORT Approach and SHE Technology Library Generation

This section focuses on implementing Boolean gates and logic circuits based on the developed SHE-based MGs (SHE-MG). To achieve this objective, we develop a SHE-based Synthesis and Optimization Routine and Tool (SHE-SORT). As shown in Figure 5.4, SHE-SORT is comprised of two modules: (1) *Developed Genetic Algorithm (GA) optimization unit*, which realizes a tree-structured Boolean expression according to the optimization criterion. The tree structure is constructed of a combination of inverters and MGs with varying numbers of inputs, and (2) *Netlist Generator*, which develops a circuit nodal topology according to the generated tree structure of the target Boolean expression. The SPICE circuit simulation tool leverages the produced optimized netlist, as well as a SHE device model to validate the functionality and estimate power and delay metrics of the realized SHE-based Boolean logic circuit.

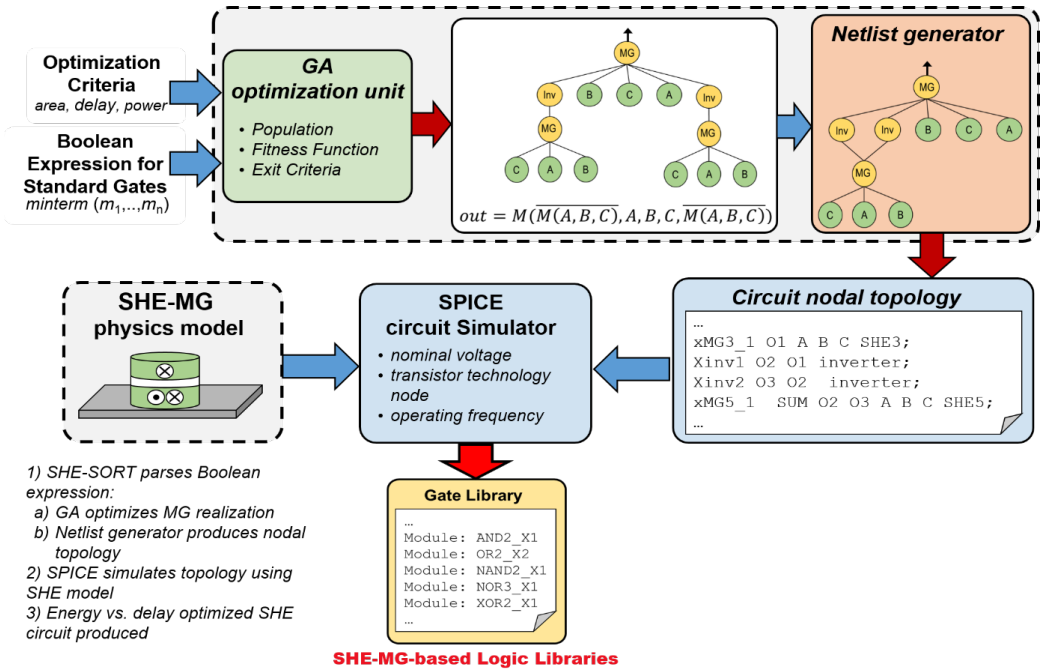


Figure 5.4: Proposed MG synthesis approach to realize SHE-based Boolean Logic, including SHE-MG based gate libraries.

The netlist generator research emphasizes methods to collapse isomorphic sub-trees into an optimized MG graph, based on the MG device libraries developed. The netlist generator outputs a SPICE syntax compatible file that can be utilized by circuit simulation toolchain in conjunction with the SHE model library to synthesize the target Boolean circuit. Hence, this developed GA-driven research synthesis tool utilizes to extract an optimized netlist for standard majority logic-based gate libraries. Our optimization methodology for spin-based NoC circuits is described, as shown in Figure 5.5. Spin-based components are utilized for storing and computing, whereas CMOS-based elements are used for implementing logic in storage elements, as well as to conduct the read operation. Required sensing scheme is provided by PCSA, which generates both output (OUT) and invert of the output ($\overline{\text{OUT}}$). Hence, the intrinsic structure of the proposed spin-based NoC cell includes one MG, which provides a functionally-complete unit. Thus, in our proposed optimization methodology, the implementation cost of the inverter gate is equal to zero. Our proposed evolutionary approach includes two levels of optimization to reduce the convergence time: Technology-Dependent Optimization and Performance Optimization.

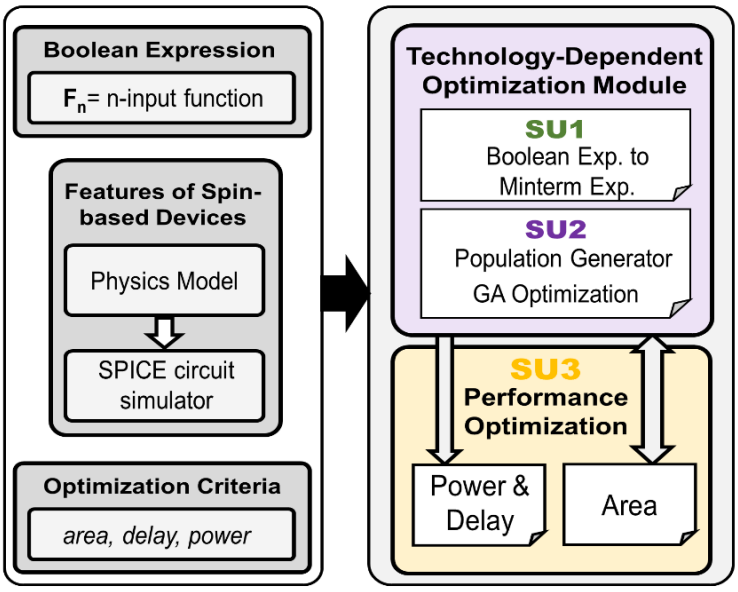


Figure 5.5: Schematic of the proposed evolutionary approach to realize MG- based NoC circuit.

Technology-Dependent Optimization

In the first level of the optimization, Genetic Algorithms (GAs) are utilized to optimize the implementation of a Boolean logic expression in terms of area, delay, or power. Although GAs were selected for the proof-of-concept framework due to their rapid prototyping ability to achieve multi-objective optimization, extensions are identified subsequently in the following sub-sections. It leverages the spin-based device characteristics as inputs to achieve a semi-optimized implementation. First, a transforming unit, which is *Synthesis Unit 1* (SU1), decomposes a Boolean expression into its minterms. Then, the generated minterm expression is applied to a mapping and optimization unit, which is SU2, along with optimization criteria and characteristics of spin-based building blocks. For instance, in a design with 3-input and 5-input spin- based MGs as building blocks, first MGs are separately implemented, and their related delay, area, and power consumption are measured. Then, the obtained results are leveraged to define their implementation cost within the optimization methodology. Finally, the GAs are utilized to optimize a Boolean logic implementation based on the optimization criteria and the obtained implementation cost of the spin-based building blocks in SU3.

GAs are biologically-inspired algorithms which are one of the most popular multi-objective tools due to their ability to empirically explore complex search spaces regardless of their gradient or higher derivatives to realize suitable designs in a design prototyping environment. As shown in Figure 5.5, the mapping and optimization unit involves three main steps as explained in the following sequence.

1) *Initialization*: an initial set of tree-based structures are created, in which each parent can have three or five random children. Each of the trees is a chromosome and the complete set is called the initial population. The GA convergence time could be adjusted by the population size and range chromosome variety. Extending the population size leads to increasing the variety of chro-

mosomes, which is limited to some upper bounds. However, this extension leads to an increase in the total processing time of GA.

2) *Fitness Evaluation*: To evolve the population toward better solutions the fitness of each chromosome is evaluated. Therefore, a fitness function is defined to assign a fitness value to the chromosomes. This evaluation is required on several occasions during the operation of the algorithm including parent selection, and constitution of the next generation population. Herein, the fitness function is expressed by $f(t_i) = N(m, t_i)/(lengthof t_i)+1/N(r, t_i)+1/(numberofgate)$, where m is the applied input minterms, $N()$ is a function that calculates the number of minterms in m, which is implemented by t_i tree, and r is the remainder of the minterms that should not be implemented. As it can be seen, the fitness function has an inverse relation with the length of the tree, which results in producing balanced trees. It enables performing a larger number of parallel operations at each level leading to power and delay optimized implementations.

3) *Replacement*: GA generates new offspring(s) from selected parents with a defined probability to achieve improved solutions to the problem. Herein, the sub-tree has been selected as the crossover operator, which selects two nodes and exchanges their sub-trees rooted from the selected nodes. Moreover, a mutation operation is performed by creating randomly generated chromosomes and exchanging them by a number of randomly selected chromosomes with a specific probability. The mutation operation is applied to avoid the algorithm being trapped in a local optimum. Tournament selection has been utilized in order to select the parents for crossover and mutation operators. The algorithm stops when no improvement in fitness function happens after more than 100 generations. The output of this mapping and optimization unit is an optimized graph expression, as shown in Figure 5.6. Algorithm 1 and Figure 5.7(a) illustrate the evolutionary approach leveraged in the proposed technology-dependent optimization methodology.

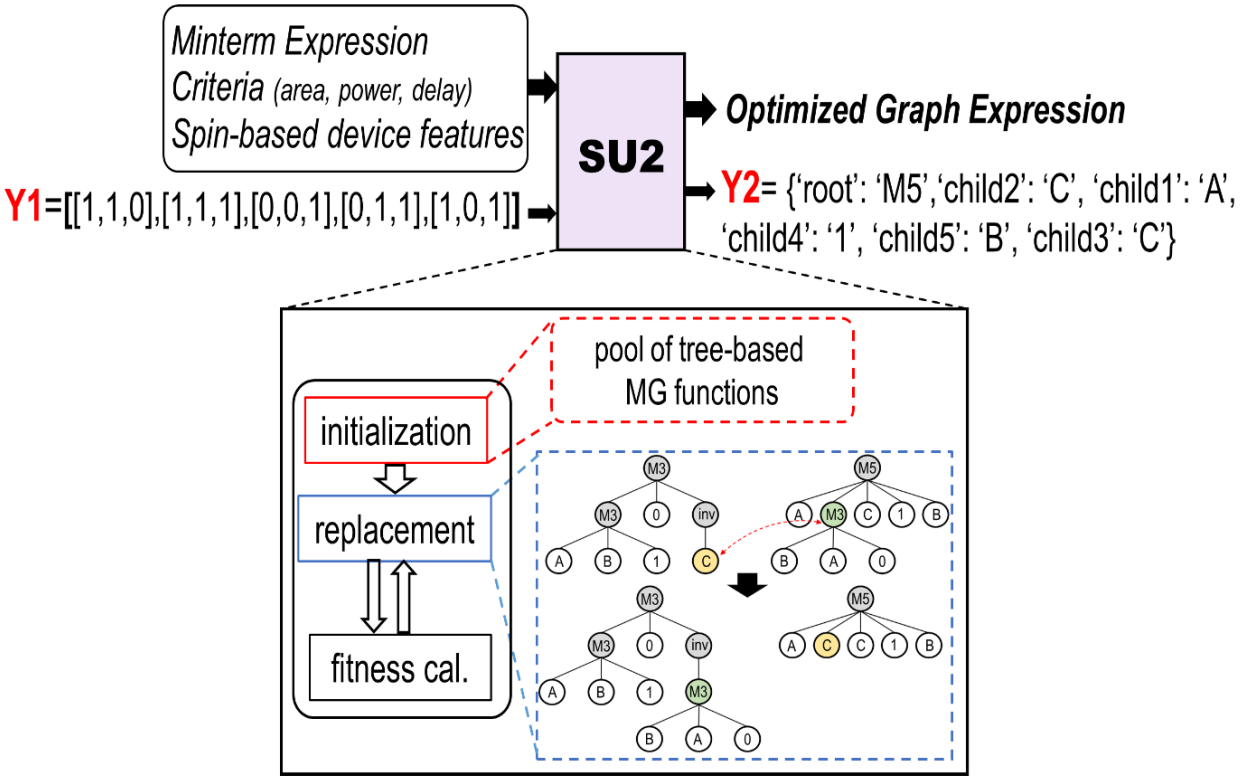


Figure 5.6: Operations of F1 and F2 blocks for AB+C in technology-dependent optimization process.

Power and Delay Optimization

The computational mechanism underlying most spintronic devices is the charge accumulation mode operation. Therefore, increasing the input current decreases the operation's delay at the expense of increased power consumption. As it was mentioned in Section 2, AND/OR gates can be readily implemented by majority gates, for instance, to realize a 2-input OR (AND) gate, one of the input transistors of a 3-input MG should be ON (OFF). Therefore, disjunction operator (OR) has larger power consumption than conjunction operator (AND), due to a higher number of ON transistors that leads to the higher input current. Since the implementation cost of an inverter is

equal to zero in our optimization methodology, disjunction operators and conjunction operators can be replaced according to the well-known De Morgans law without any redundancy cost. Hence, a third functional unit (SU3) is added to the optimization tool, which replaces the OR (AND) operations by AND (OR)-inverter operations within the logic implementation to reduce power (delay). Algorithm 2 describes SU3 functionality, which first takes the optimized tree obtained by SU2.

Algorithm 1 Mapping and Optimization Algorithm

procedure TRANSFORMING(1)
    Input: Boolean Expression (Gate functionality)
    Generate truth table of an applied n-input function
    Convert Boolean expression to minterms
    Output: Minterms expression set
end procedure
procedure MAPPING AND OPTIMIZATION ALGORITHM
    Input$_1$: Generated minterms
    Input$_3$: Optimization criteria (area, delay, power)
    Step1: *Initialization*
    Define implementation cost for 3-input MG (M3) and 5-input MG (M5)
    Adjust optimization factor based on cost and applied criterion
    Generate a pool of tree-based MG functions
    Label root with M3 (M5) & add a node with respect to root
    Step2: *Fitness Evaluation*
    $f(t_i) = \frac{N(m,t_i)}{(length(t_i))} + \frac{1.0}{N(r,t_i)+1} + \frac{1.0}{\#gate+1}$
    Compute $f(t_i)$ for the constructed tree t_i
    if progress in f is less than threshold **or** constraint on the upper limit number of generations is reached **then**
        Break
    end if
    Step3: *Crossover*
    P_1, P_2= Randomly select two branches from different trees
    if root (P_1) & root (P_2) are M3 or M5 **then**
        Replace selected sub-trees with each other
    else
        Repeat Step3 until reach a leaf then Break
    end if
    Repeat Step2
    Output: Optimized graph expression
end procedure

Algorithm 2 Power Optimization

```
1: Input: Technology-Dependent Optimized tree (t)
2: procedure PRE_ORDER_TRAVERSAL (T)
3:     while t is not NULL do
4:         if t is tree then
5:             x ← root(t)
6:             if x == (M3 or not M3) then
7:                 for j in 3 do
8:                     pre-order traversal (sub-tree j)
9:                 end for
10:            else if x== (M5 or not M5) then
11:                for j in 5 do
12:                    pre_order_traversal (sub-tree j)
13:                end for
14:            end if
15:        else
16:            x ← value(t)
17:            if x==1 then
18:                Update (invert) all children with parent(x)
19:                Select OUT instead of OUT (vice versa) to output
20:            end if
21:            return
22:        end if
23:    end while
24: end procedure
25: Output: Power optimized tree
```

Then, it executes a pre-order traversal scheme to visit a node, check its value, and update it, recursively. All of the trees or sub-trees with a root labeled M3 or M5 are examined to find any leaf with value "1". Then, it replaces "1" with "0" and inverts all of the remaining leaves with the same parent. Finally, it uses the OUT signal instead of OUT to invert the whole tree or subtree. An example of a power-optimized implementation of (A+B+C+D) expression and its corresponding normalized simulation results are shown in Figure 5.7(b) and Figure 5.7(d), respectively.

Area Optimization

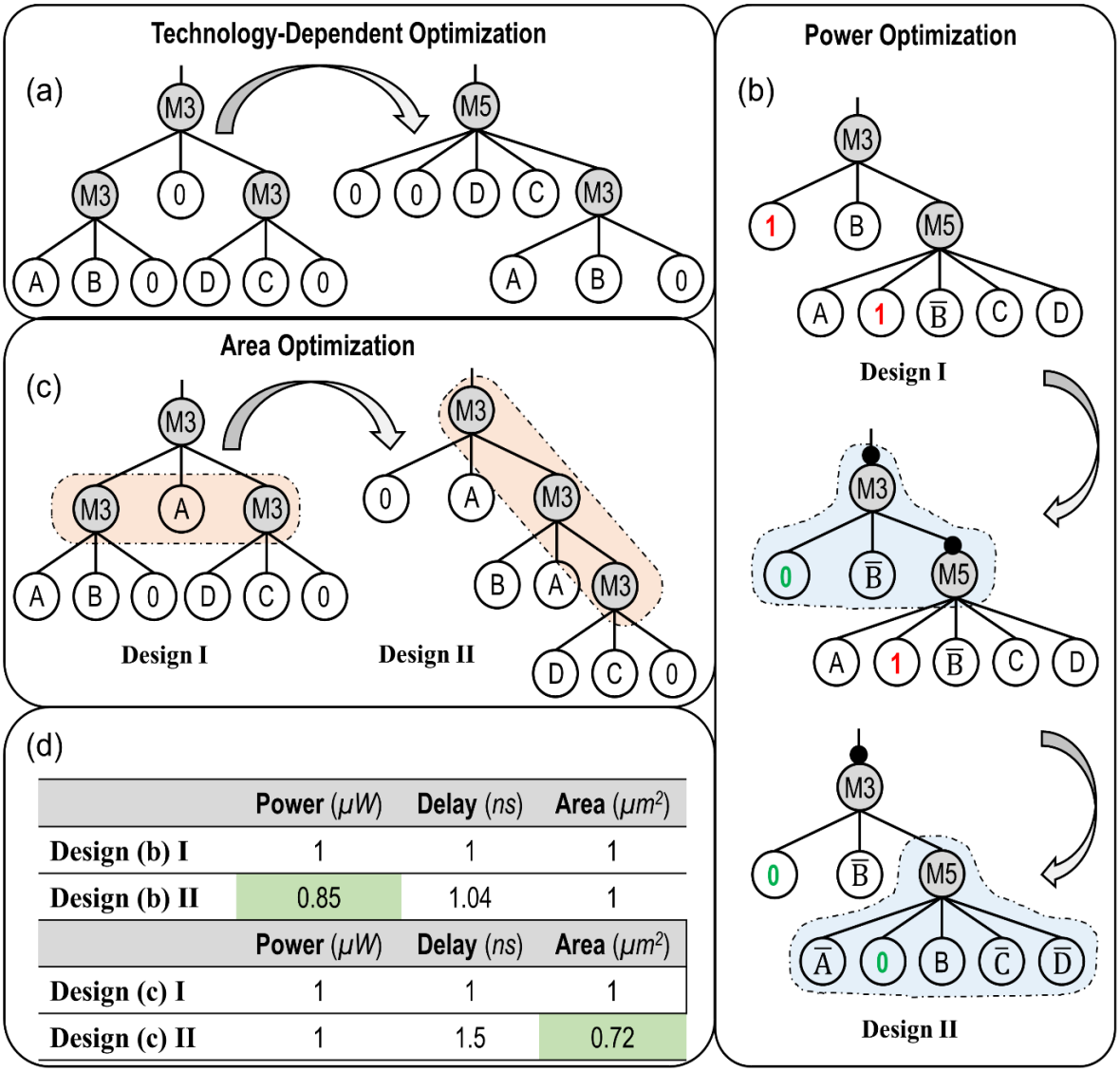
In the proposed NoC architecture each MG node requires one PCSA. Therefore, the number of PCSAs required for each layer depends on the number of MG nodes existing in that non-volatile spintronic layer. On the other hand, PCSAs can be shared between different non-volatile spintronic layers. Thus, the number of PCSAs required for implementing an NoC circuit is equal to the maximum number of MG nodes utilized in any non-volatile spintronic layer. However, According to the fitness function described previously, trees with balanced structure have larger fitness value. Although the balanced tree structure, e.g. shown in Design I of Figure 5.7(c), provides an optimized implementation in term of delay or power consumption, it requires a larger number of PCSAs due to having more MG nodes in second layer leading to higher area overhead. Hence, for area optimization we have modified the fitness function to $f(t_i) = N(m,t_i)/(lengthof t_i) + 1/N(r,t_i) + 1/(numberofgate) + 1/(nMG+1)$, where nMG is the maximum number of PCSAs in the implemented design. The procedure leveraged a breadth-first search technique to find the maximum number of MGs in one level. Therefore, the optimization methodology creates an unbalanced tree with less number of MG nodes in each layer as shown in Design II of Figure 5.7(c). Thus, only a single PCSA is required to implement the A(B+CD) Boolean expression, which results in decreased area consumption while increasing delay, as shown in Figure 5.7(d). This is caused by the increased sequential operations required to deliver the output of each logic layer to the next one.

Simulation Results

In this section, we have leveraged our proposed optimization methodology to implement a functionally-complete set of Boolean logic gates using SHE-MTJ, as a proof-of-concept for an optimized spin-based NoC circuit design. Herein, the developed SHE-MTJ cells are utilized to implement stan-

dard functions. In accordance with Figure 5.3, PMOS transistors are leveraged to produce the input charge currents, while a PCSA is used to sense the SHE-MTJs' states. The dimensions of the 3-input (5-input) SHE-MG is designed in a manner such that at least two (three) out of the three (five) input transistors should be ON to produce a current amplitude greater than the critical current of SHE-MTJ. Switching the 5-input SHE-MG requires a larger number of ON transistors leading to higher input charge current which increases the power consumption, while decreasing switching delay [135].

To implement spin-based NoC cells, the 3-input and 5- input SHE-MGs are defined as functional blocks and their characteristics are applied to the optimization tool. The proposed evolutionary approach is leveraged to implement a functionally-complete set of Boolean logic gates. For each of the Boolean functions, power and area optimization resulted in an identical implementation, while the delay optimization generated a different implementation. As listed in Table 5.4, there is a higher number of "0" inputs in power-optimized structures, while delay-optimized implementations include more "1" inputs. This is achieved by the performance optimization method introduced in Section 3, which leads to smaller input current for power-optimized and larger input current for delay-optimized implementations. Moreover, Figure 5.8 exhibits the normalized power dissipation and delay for selected 2-input to 6- input Boolean logic circuits, which are implemented using the proposed power-optimization and delay-optimization paradigms. The results verify the efficiency of our optimization methodology for NoC circuit implementations.



	Power (μW)	Delay (ns)	Area (μm^2)
Design (b) I	1	1	1
Design (b) II	0.85	1.04	1

	Power (μW)	Delay (ns)	Area (μm^2)
Design (c) I	1	1	1
Design (c) II	1	1.5	0.72

Figure 5.7: (a) technology-dependent optimization for F= A.B.C.D, (b) power optimization for F= A+B+C+D, (c) area optimization for F= A(B+CD), and (d) comparison results for Designs in (b) and (c).

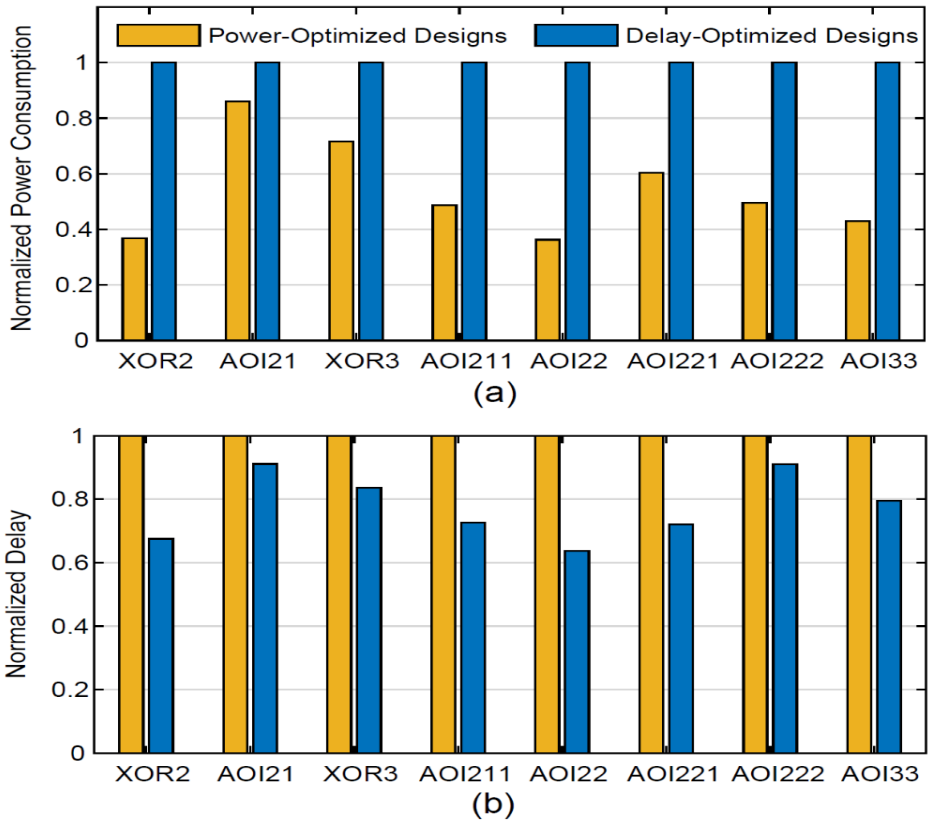


Figure 5.8: Normalized results for (a) power consumption, and (b) delay leveraging two optimization approaches.

Table 5.4: Optimized implementation of the functionally-complete set of Boolean logic gates using SHE-MGs.

Standard Functions	**Efficiency Criteria**	
	Power*	**Delay**
1. A.B (or $\overline{\mathrm{A.B}}$)	**M**(A,B,0)	$\overline{\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, 1, 0, 1)}$
2. A+B (or $\overline{\mathrm{A}+\mathrm{B}}$)	$\overline{\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, 0)}$	**M**(A,B,0,1,1)
3. $\overline{\mathrm{A}}$.B+A.$\overline{\mathrm{B}}$ (or $\overline{\mathrm{A}}$.$\overline{\mathrm{B}}$+A.B)	$\overline{\mathbf{M}(\overline{\mathbf{M}(\overline{\mathrm{A}}, \mathrm{B}, 0)}, \overline{\mathbf{M}(\overline{\mathrm{B}}, \mathrm{A}, 0)}, 0)}$	$\overline{\mathbf{M}(\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{A}, \mathrm{B}, 1)}, \overline{\mathrm{B}}, \overline{\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, \overline{\mathrm{B}}, 1, \overline{\mathrm{A}})}, \mathrm{B}, 1)}$
4. A.B.C (or $\overline{\mathrm{A.B.C}}$)	**M**(A,B,C,0,0)	$\overline{\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, \overline{\mathrm{C}}, 1, 1)}$
5. A+B+C (or $\overline{\mathrm{A}+\mathrm{B}+\mathrm{C}}$)	$\overline{\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, \overline{\mathrm{C}}, 0, 0)}$	**M**(A,B,C,1,1)
6. $\overline{(\mathrm{A.B})+\mathrm{C}}$	**M**($\overline{\mathrm{A}}$,$\overline{\mathrm{B}}$,$\overline{\mathrm{C}}$,$\overline{\mathrm{C}}$,0)	$\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{C}, 1)}$
7. $\overline{(\mathrm{A}+\mathrm{B}).\mathrm{C}}$	$\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{C}, 0)}$	**M**($\overline{\mathrm{A}}$, $\overline{\mathrm{B}}$, $\overline{\mathrm{C}}$, $\overline{\mathrm{C}}$,1)
8. A.$\overline{\mathrm{C}}$+B.C	**M**(**M**($\overline{\mathrm{A}}$, $\overline{\mathrm{C}}$, 0)**M**(0,B,C),$\overline{\mathrm{C}}$)	**M**(A,B,$\overline{\mathbf{M}(\overline{\mathrm{B}}, \overline{\mathrm{C}}, \mathrm{A}, 1, 1)}$,**M**(1,$\overline{\mathrm{B}}$,1,A,C),$\overline{\mathrm{C}}$)
9. A.B+B.C+A.C	**M**(A,B,C)	**M**(A,B,C,1,0)
10. A$\oplus$B$\oplus$C	**M**(**M**(A,B,$\overline{\mathrm{C}}$),C,$\overline{\mathbf{M}(\mathrm{B}, \mathrm{A}, \mathrm{C})}$)	**M**(A,$\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{C}, 0, 1)}$,**B**,**C**, $\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{C}, 0, 1)}$)
11. A.B.C.D (or $\overline{\mathrm{A.B.C.D}}$)	**M**(D,0,**M**(A,B,$\overline{\mathrm{D}}$,C,0))	$\overline{\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{D}}, 1, 1, \overline{\mathbf{M}(\mathrm{A}, \overline{\mathrm{B}}, \overline{\mathrm{C}}, \overline{\mathrm{D}}, 1)})}$
12. A+B+C+D (or $\overline{\mathrm{A}+\mathrm{B}+\mathrm{C}+\mathrm{D}}$)	$\overline{\mathbf{M}(\overline{\mathrm{B}}, 0, \mathbf{M}(\overline{\mathrm{A}}, \mathrm{B}, \overline{\mathrm{C}}, \overline{\mathrm{D}}, 0))}$	**M**(C,1,**M**($\overline{\mathrm{C}}$,B,A,1,D),$\overline{\mathrm{B}}$,B)
13. $\overline{(\mathrm{A.B}+\mathrm{C}+\mathrm{D})}$	**M**($\overline{\mathrm{C}}$,0,**M**($\overline{\mathrm{A}}$,$\overline{\mathrm{B}}$,$\overline{\mathrm{D}}$,$\overline{\mathrm{D}}$,0))	$\overline{\mathbf{M}(\mathrm{C}, \mathrm{D}, 1, 1, \mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{D}, \mathrm{C}, 1))}$
14. $\overline{(\mathrm{A}+\mathrm{B}).\mathrm{C}.\mathrm{D}}$	$\overline{\mathbf{M}(0, \mathrm{C}, \mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{D}, \mathrm{D}, 0))}$	$\overline{\mathbf{M}(\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, \overline{\mathrm{C}}, \overline{\mathrm{D}}, 1), \overline{\mathrm{C}}, \overline{\mathrm{D}}, 1, 1)}$
15. $\overline{(\mathrm{A.B}+\mathrm{C.D})}$	**M**($\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, 0)}$,$\overline{\mathbf{M}(\mathrm{C}, \mathrm{D}, 0)}$,0)	$\overline{\mathbf{M}(\mathrm{C}, \overline{\mathbf{M}(1, 1, 0, \overline{\mathrm{A}}, \overline{\mathrm{B}})}, \overline{\mathbf{M}(1, \mathrm{C}, \mathrm{D}, \overline{\mathrm{A}}, \overline{\mathrm{B}})}, \mathrm{D}, 1)}$
16. $\overline{(\mathrm{A}+\mathrm{B}).(\mathrm{C}+\mathrm{D})}$	**M**($\overline{\mathbf{M}(\mathrm{A}, \overline{\mathrm{B}}, 0)}$,$\overline{\mathrm{B}}$,**M**(0,$\overline{\mathrm{C}}$,$\overline{\mathrm{D}}$))	**M**($\overline{\mathrm{A}}$,$\overline{\mathrm{B}}$,**B**,**M**($\overline{\mathrm{B}}$, $\overline{\mathrm{B}}$, $\overline{\mathrm{C}}$, $\overline{\mathrm{D}}$, 1),**M**(A,**B**,$\overline{\mathrm{C}}$,$\overline{\mathrm{D}}$,1))
17. $\overline{(\mathrm{A.B}+\mathrm{C.D}+\mathrm{E})}$	**M**($\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{E})}$,0,**M**($\overline{\mathrm{C}}$, $\overline{\mathrm{D}}$, $\overline{\mathrm{E}}$, $\overline{\mathrm{E}}$, 0))	**M**(E,$\overline{\mathrm{E}}$,1,$\overline{\mathbf{M}(\mathrm{B}, \mathrm{A}, \mathrm{E}, \overline{\mathrm{E}}, \overline{\mathrm{E}})}$,**M**(C,1,D,E,E))
18. $\overline{(\mathrm{A}+\mathrm{B}).(\mathrm{C}+\mathrm{D}).\mathrm{E}}$	$\overline{\mathbf{M}(\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{E}), 0, \mathbf{M}(\mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{E}, 0))}$	**M**(E,$\overline{\mathrm{E}}$,1,**M**($\overline{\mathrm{C}}$, $\overline{\mathrm{D}}$, $\overline{\mathrm{E}}$, 1, $\overline{\mathrm{E}}$),**M**(B,A,E,$\overline{\mathrm{E}}$,$\overline{\mathrm{E}}$))
19. $\overline{(\mathrm{A.B}+\mathrm{C.D}+\mathrm{E.F})}$	**M**($\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, 0)}$, $\overline{\mathbf{M}(\mathrm{C}, \mathrm{D}, 0)}$, $\overline{\mathbf{M}(\mathrm{E}, \mathrm{F}, 0)}$,0,0)	$\overline{\mathbf{M}(\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, 1)}, \overline{\mathbf{M}(\overline{\mathrm{C}}, \overline{\mathrm{D}}, 1)}, \overline{\mathbf{M}(\overline{\mathrm{E}}, \overline{\mathrm{F}}, 1)}, 1, 1)}$
20. $\overline{(\mathrm{A}+\mathrm{B}).(\mathrm{C}+\mathrm{D}).(\mathrm{E}+\mathrm{F})}$	$\overline{\mathbf{M}(0, \mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, 0), \overline{\mathbf{M}(\overline{\mathrm{C}}, \overline{\mathrm{D}}, 0)}, 0, \overline{\mathbf{M}(\overline{\mathrm{E}}, \overline{\mathrm{F}}, 0)})}$	**M**(1,$\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, 1)}$, $\overline{\mathbf{M}(1, \mathrm{C}, \mathrm{D})}$, 1, $\overline{\mathbf{M}(\mathrm{E}, 1, \mathrm{F})}$)
21. $\overline{(\mathrm{A}+\mathrm{B}+\mathrm{C}).(\mathrm{D}+\mathrm{E}+\mathrm{F})}$	$\overline{\mathbf{M}(\mathbf{M}(\overline{\mathrm{A}}, \overline{\mathrm{B}}, \overline{\mathrm{C}}, 0, 0), 0, \mathbf{M}(\overline{\mathrm{D}}, \overline{\mathrm{E}}, \overline{\mathrm{F}}, 0, 0))}$	**M**(0,1,$\overline{\mathbf{M}(\mathrm{A}, \mathrm{B}, \mathrm{C}, 1, 1)}$, 1, $\overline{\mathbf{M}(\mathrm{D}, \mathrm{E}, \mathrm{F}, 1, 1)}$)

($*$) Power and area optimization resulted in an identical implementation.

NV-Clustering Design Methodology

Herein, we develop a standardized methodology to synthesize optimized NV architectures, which is referred to as NV-Clustering[2]. NV-Clustering selectively collects together compatible Boolean logic functions and state holding functions, as depicted in Figure 5.9. It utilizes: (1) LE-FFs as NV storage elements that also serve as computational elements, (2) a methodology for utilizing the developed cells to achieve robust intermittent operation, and (3) a constraint-based optimization step considering area, power, and delay to realize a preferred NV-enhanced datapath design.

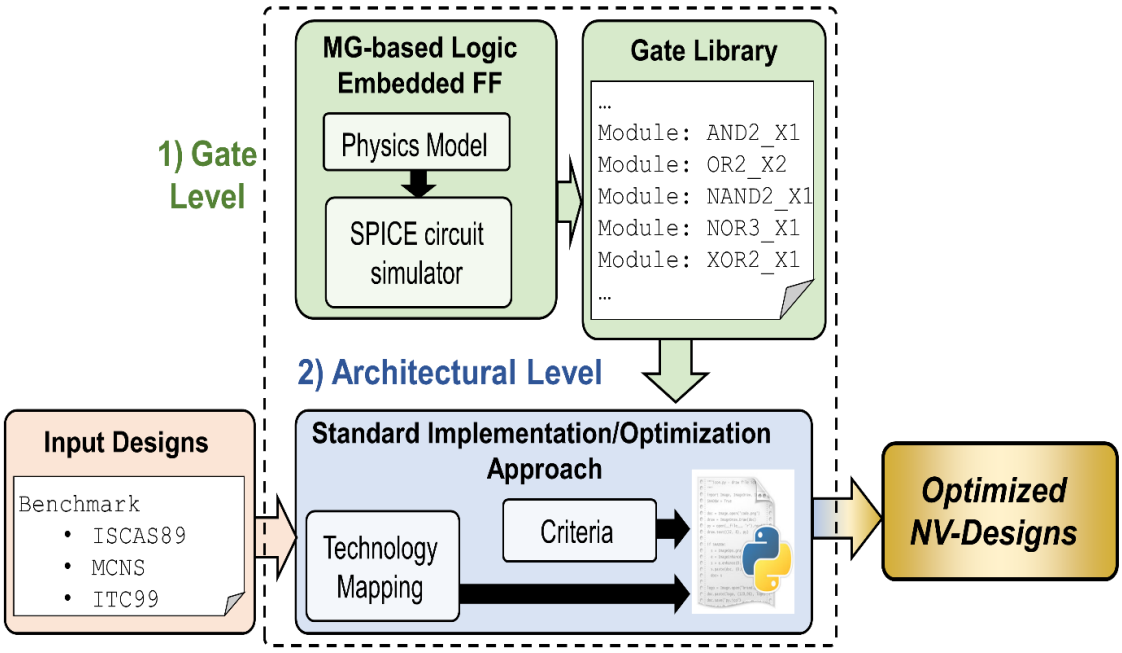


Figure 5.9: Optimized NV implementation methodology diagram.

[2]©2018 IEEE. Reprinted, with permission, from [123].

Logic-Embedded FF (LE-FF) Design

Based on the explanation of the operation of spintronic devices in Section 2, the unifying computational mechanism underlying MTJ-based devices is an accumulation-mode operation that enables the realization of Majority Gates (MG) as basic computational building blocks. In an n-input MTJ-based MG (MTJ-MG), the device is designed such that when at least (n-1)/2 of the inputs are asserted to logic 1 (ON), then a switching current greater than the critical current is produced. A pre-charge sense amplifier (PCSA) [136] is utilized to sense the state of the MTJs, which generates both the output and the inverted output ($\overline{output}$). Therefore, MTJ-MG cells can provide a functionally-complete set of Boolean logic expressions. Since an MTJ-MG functional block is an NV element, it can retain a value similar to a clocked FF. Hence, our proposed LE-FF is composed of a spin MG-based master latch and a CMOS-based slave latch, as shown in Figure 5.10(a). The LE-FF is comprised of a master latch realized by a SHE-MTJ NV device, a slave latch, and a PCSA. A LE-FF has three different modes: store mode, in which the write operation to NVM is performed; *standby mode*, in which the power is disabled; and *sense mode*, in which the stored data in NVM is read. After power-up, the data is restored into the slave latch. Therefore, due to its non-volatility, the entire design can be power gated without incurring vulnerability to the datapath. It is able to compute operation and also store value during the first cycle, whereas the output, Q, is propagated during the second cycle.

Our proposed LE-FF has two significant features in comparison to the previously presented NV-FF designs: (a) in addition to storing a value with nearly-zero standby power, similar to the other NV-FFs, the LE-FF design is capable of computing rudimentary Boolean expressions intrinsically, resulting in area, complexity, and power reduction. For instance, by affixing one (or two) of the three (or five) input transistors to ON or OFF states upon demand during the circuit operation, then a 2(or 3)-input OR gate or a 2(or 3)-input AND gate can be realized, respectively. Figure

5.10(b) shows a 2-input OR which is connected to an NV-FF and its equivalent implementation using LE-FF. Table 5.5 summarizes all possible Boolean expression, which can be implemented using 3- and 5- input LE-FFs. Their implementation capacities might be enhanced by leveraging larger MGs. Moreover, (b) by using LE-FFs, the implemented designs have lower sensitive time to power failures. It is determined by the duration of signal propagation between two NV elements including: (1) input registers and an NV-FF, (2) two NV-FFs, or (3) an NV-FF and output registers, in which if a power failure occurred, data will be lost and rebooting required. Figure 5.11 depicts all three possible durations. The vulnerability interval is expressed by equation 5.1:

$$t_s = t_{WR} + t_{RD} + t_D \tag{5.1}$$

where, t_{WR} is the write operation time for the NV element, t_{RD} is the switching time of CMOS-based latches, e.g. a master latch, and t_C is the required time for combinational circuits before storing into NV-FFs, as shown in Figure 5.11. In a datapath, the summation of all obtained sensitive time is considered as a design vulnerability time (DVT), which implies that a design with a smaller DVT provides higher tolerance to power failure. Hence, replacing cones of gates and NV-FFs by LE-FFs will reduce DVT, increasing failure robustness, which improves redundant restart efficiency. In order to design optimized NV architectures using the proposed LE-FF, there is a need to develop a systematic methodology, which incorporates all LE-FF features to design power-failure tolerant architectures. The developed approach leverages the maximum capability of LE-FFs in terms of replacement and implementation steps.

Table 5.5: Boolean Expressions using 3 and 5 -input MGs.

Majority Gate	Inputs A	B	C	D	E	Equivalent Functionality
3-input MG	a	b	c	-	-	3-input MG
	a	b	0	-	-	2-input AND gate*
	a	b	1	-	-	2-input OR
5-input MG	a	b	c	d	e	5-input MG
	a	b	c	0	0	3-input AND gate
	a	b	c	1	1	3-input OR gate
	a	b	c	c	0	OAI21
	a	b	c	c	1	AOI21

*It generates both out and invert of the out, i.e. AND and NAND.

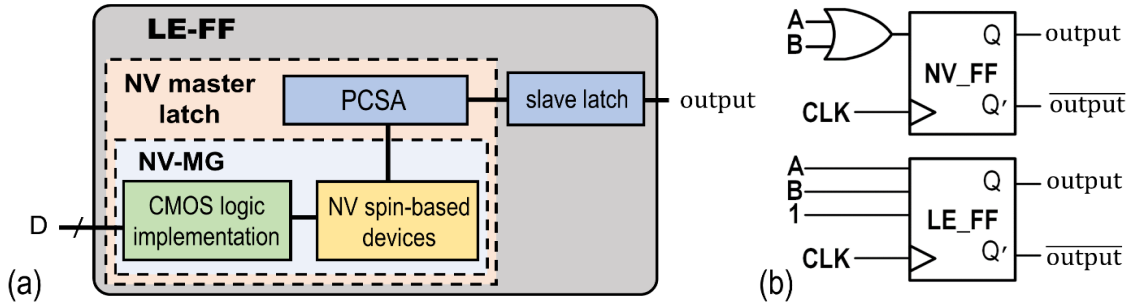


Figure 5.10: (a) Schematic of proposed MG-based LE-FF, and (b) different implementations using NV-FF (top), and proposed LE-FF (bottom).

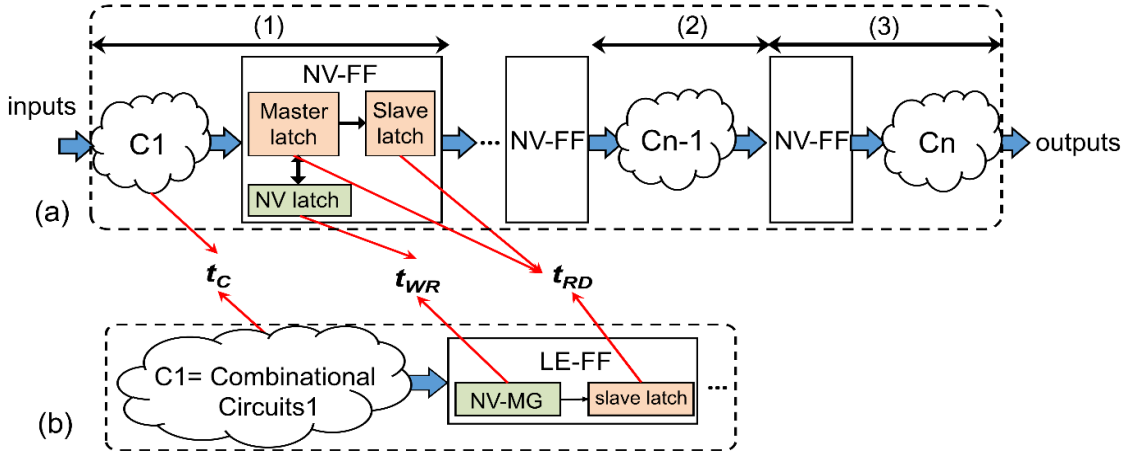


Figure 5.11: All three sensitive time durations for (a) NV-FF based implementation, and for (b) proposed implementation approach, in which C1(b) < C1(a).

NV-Clustering Methodology

In this subsection, we define the proposed NV-Clustering methodology. It takes a hardware description language (HDL) representation of a datapath and MG-based gate modules as its inputs and produces an optimized NV-enhanced datapath.

The proposed methodology was constructed in Python, according to the control flow illustrated in Algorithm 3. Its three primary procedures are: (1) **`find_gate(X)`** which finds a gate generating the output **`X`**, (2) **`find_input(Y)`** which finds all the primary inputs of gate **`Y`**, and (3) **`check(Z)`** which validates correctness according to the following circuit-level criteria regarding gate list **`Z`** :

Criterion#1: All gates in list **`Z`** are implemented by exactly one LE-FF. Rationale: Whereas each LE-FF requires one clock cycle for computation and to ensure the functional correctness of the design, the list **`Z`** including a cone of combinational logic gates and a master latch has a tight bound to occur within one clock cycle. Hence, the use of more than one MG for complex functions could increase the propagation delay enough to violate timing constraints. Hence, all elements in the list should be implemented using one LE-FF.

Criterion#2: Fan-out of every gate in list **`Z`** cannot exceed one. Rationale: Whereas LE-FFs realize sequential designs, which implies outputs are obtained after a delay of two clock cycles, one for computation/storing (master layer), and one for reading (slave layer). If a computational circuit connects to more than one gate, then two gates which are driven, require output1 and output2 as their inputs without any delay. Therefore, implementing a clockless design is permitted iff the combinational function has fan-out of one that is driven into a single sequential block.

In addition to the abovementioned conditions, two more crucial considerations will be checked:

Criterion#3: An item in the *input_list* should not be a primary input. Rationale: If the input port is one of the primary inputs of design, it cannot be an output of a gate; hence, it is removed from the input list.

Criterion#4: The item should not be an FF's output. Rationale: If the FFs output is in the *input_list*, the possible cone-gates contain two FFs that requires two clock cycles instead of one, which causes a timing violation. Hence, the input is removed from the list. Therefore, due to the timing criterion, each of the cone-gates should include only one FF and one (several) combinational gate(s).

If all criteria are satisfied, then a cone of gates including all gates connected to an FF is replaced by exactly one LE-FF. Otherwise, the FF is replaced by a logic-free NV-FF. Then, the HDL code is updated based on the changes. These steps are performed for all FFs in the candidate design. Finally, the optimized HDL code is produced.

To exemplify the functionality of the proposed methodology, the s27 circuit from the ISCAS-89 benchmark is analyzed, as shown in Figure 5.12(a). The following steps are performed:

1) All FFs are listed, FF_list = {FF#1, FF#2, FF#3}

For FF#1:

STEP 1. **`create_cone`** (FF#1) is invoked. Next, **`find_input`** (FF#1) only returns **`X1`** as primary inputs and neglects the clock input. Thus, it satisfies both C3 and C4 conditions. This implies **`input_list`** = {**`X1`**}.

STEP 2. List of inputs has only one item. The **`find_gate`** (**`X1`**) function returns **`INV1`**, in which **`X1`** is its output. The **`cone_gates`** list is updated with **`INV1`**, thus **`cone_gates`** = {**`INV1`**}.

STEP 3. The function **`check`** (cone_gates) returns TRUE because **`INV1`** satisfies criteria C1 and C2. Therefore, **`INV1`** is retained in the cone.

STEP 4. Function **create_cone** (INV1) is invoked which performs all steps 1, 2, and 3. The **find_input**(INV1) returns **X2**, after checking criteria. Next, **input_list** is updated to {**X2**}. Thus, **find_gate**(X2) returns **OAI21** gate, which is appended in the **cone_gates** list as {**INV1, OAI21**}. Meanwhile, **check**(cone_gates) is still TRUE, whereas all gates can be implemented by one MG, simultaneously and each gate has fan_out of one. Thus, **create_cone**(OAI21) is invoked.

STEP 5. Invoking **create_cone**(OAI21) implies that **input_list** equals to {**X3, X4, X5**}. Meanwhile, **X3** violates the C4 condition corresponding to the output of the FF, so it is removed from the input list. Moreover, **X4** violates the C3 condition, the primary input of the circuit, thus **input_list=X5**. Accordingly, **find_gate**(X5) returns **INV2**, thus the revised set of cone_gates= {INV1, OAI21, INV2}. Since cone_gates satisfies C1 and C2 criteria, **check**(cone_gates) returns TRUE. Hence, **create_cone**(INV2) is invoked.

STEP 6. Invocation of **create_cone**(INV2) generates input_list=**X6**. However, X6 violates criterion C3. Then **cone_gates** returns to the main procedure. If its cardinality exceeds one, then the replaceable combinational gates are specified in **cone_gates** while the FF is replaced by a LE-FF. Otherwise, the FF is replaced by a conventional NV-FF. In this case, the HDL code becomes updated accordingly.

For FF#2:

STEP 1. Initially, **create_cone**(FF#2) is invoked, thus **find_input**(FF#2) returns **Y1**, which satisfies criteria C3 and C4. Accordingly, input_list = {**Y1**}.

STEP 2. The **find_gate**(**Y1**) function returns NOR1. The cone_gates set is updated such that cone_gates=NOR1.

STEP 3. The function **check**(cone_gates) returns TRUE whereas NOR1 satisfies criteria C1 and

C2. Therefore, NOR1 is retained in the cone.

STEP 4. Function **create_cone**(NOR1) is invoked such that input_list={Y2,Y3}. However, Y2 and Y2 violate criteria C2 whereas both gates fan-out of 2. Thus, cone_gates is returned to the main procedure and because it is non-null, whereby the FF and NOR gates become replaced by LE-FF. The HDL code is updated accordingly.

For FF#3:

STEP 1. Procedure **create_cone**(FF#3) is invoked resulting in **find_input**(FF#3) returning Z1. It violates criterion C2. Thus, **cone_gates** is returned to the main procedure, and because of an empty list, the FF is replaced by a conventional NV-FF. Whereas FF_list is empty, it outputs the optimized HDL code. The optimized schematic for s27 is shown in Figure 5.12(b), which is discussed below.

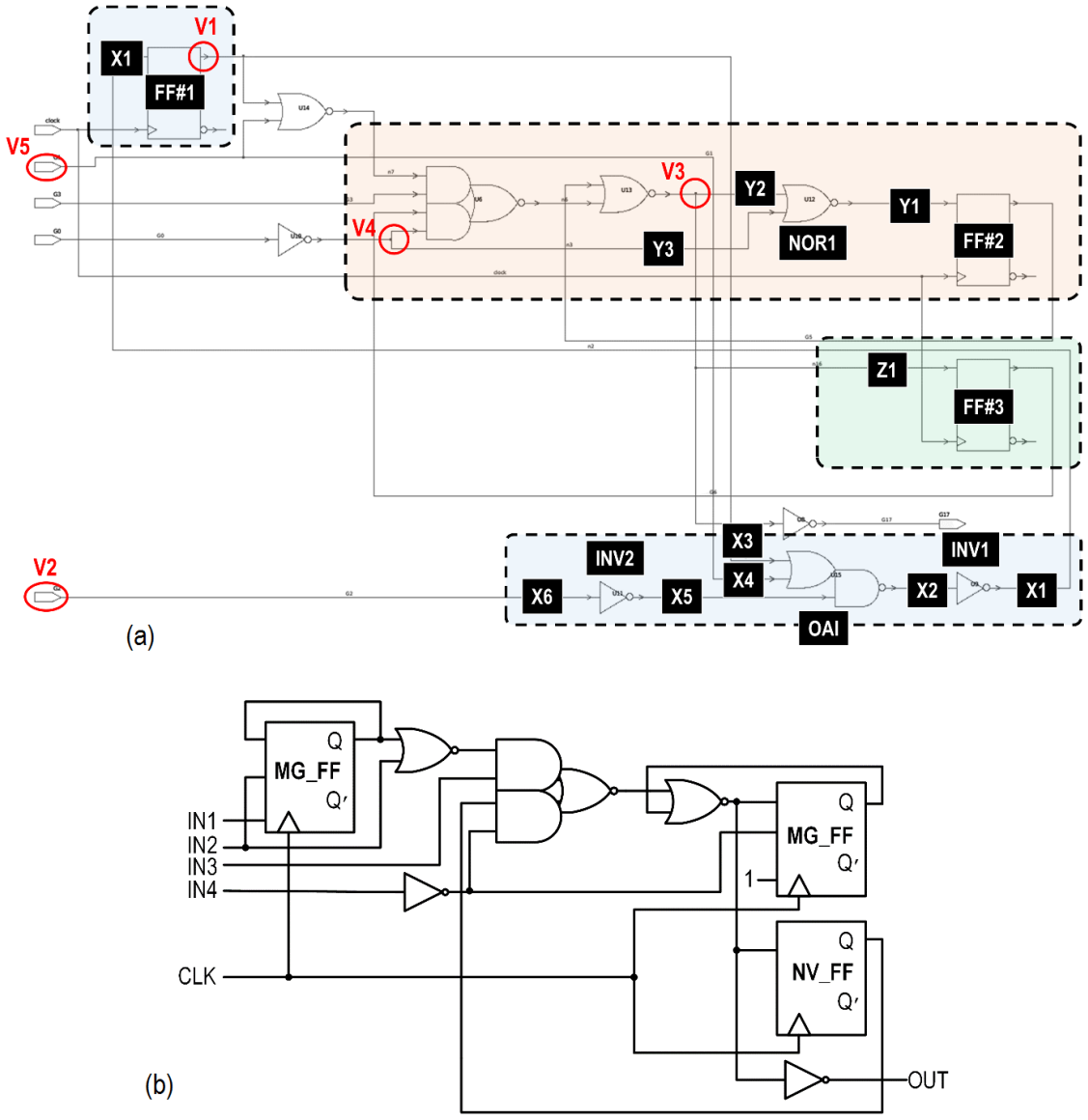


Figure 5.12: (a) s27 schematic with highlighted FFs, and (b) optimized LE-FF based design after NV-Clustering.

Simulation Results

In this Section, performance characteristics, including power, delay, and area of NV-Clustering are elaborated. First, non-volatile SHE-MTJ-based MG libraries were constructing using our model developed as a case study. The circuit implementation of a 3-input SHE-based LE-FF is depicted in Figure 5.13(a). It consists of an NV master latch comprised of the write circuitry, one SHE-MTJ as an NV element, as well as a PCSA, and a CMOS-based slave latch. LE-FF functionality is verified by circuit simulation using the SPICE for outputs depicted in Figure 5.13(b). First, the state of SHE-MTJ is in the parallel (P) configuration. The applied inputs ABC= "001" produces charge current equals $|-56|$ μA, which is smaller than SHE-MTJ critical current, i.e., $I_{Critical}$=108 μA. Thus, the free layer (FL) magnetization direction of the SHE component remains in the P state, which in the next cycle, denotes binary 0 as an output of the slave latch. Then, the input is set to "111". The generated current is equal to 196 μA, which results in changing the FL state from a P state to an anti-parallel (AP) state, and thus, the slave latch outputs one in the next cycle. The third and fourth cycles show its functionality in the presence of power failure and power-up situations, respectively. Due to the non-volatility of the design, the FL configuration remains AP, which verifies the desired forward progress of the designs operation while supporting intermittent operation.

We developed 3-input and 5-input LE-FF libraries, which contain a functionally-complete set of Boolean logic gates. The generated libraries are utilized in a commercial synthesis tool, i.e. Synopsys design compiler, to map the produced optimized HDL code to a LE-FF based design. For instance, Table 5.6 summarizes the comparison results for CMOS-based and two different non-volatile implementations of the s27 circuit. It includes 3 FFs and 9 gates including inverters.

NV-Clustering achieves better performance based on metrics of power and area overhead, DVT, and complexity as measured using gate count. The DVT of LE-FF implementation exhibits a

reduced DVT compared to conventional NV-FF realization. This is because NV-Clustering reduces the t_C component in Equation (1), while t_{RD} is equal to the access time of the slave latch alone. Whereas in the conventional NV-FF based design, t_{RD} is calculated for both CMOS-based master and slave latches. Generally, for NV-Clustering, t_{RD} is always less than that of an NV-FF-based design. In the worst case scenario where no clustering is performed then it is reasonable to assume an identical DVT for either realization of the datapath. In other cases, LE-FF based realizations achieve a reduced DVT.

Table 5.6: Gate Counts for s27 Benchmark Circuit.

`s27` Design	Power (μW)	Gate count	Area (μm^2)	DVT
CMOS-based	1.45	9	23.33	N/A
NV-FF-based	18.6	9	24.70	359
LE-FF based	16.7	5	20.90	315

In the following sub-section, the developed libraries are leveraged to implement large scale benchmarks (**ISCAS-89**, **ITC-99**, and **MCNC**) in order to validate the functionality and performance of the NV-Clustering.

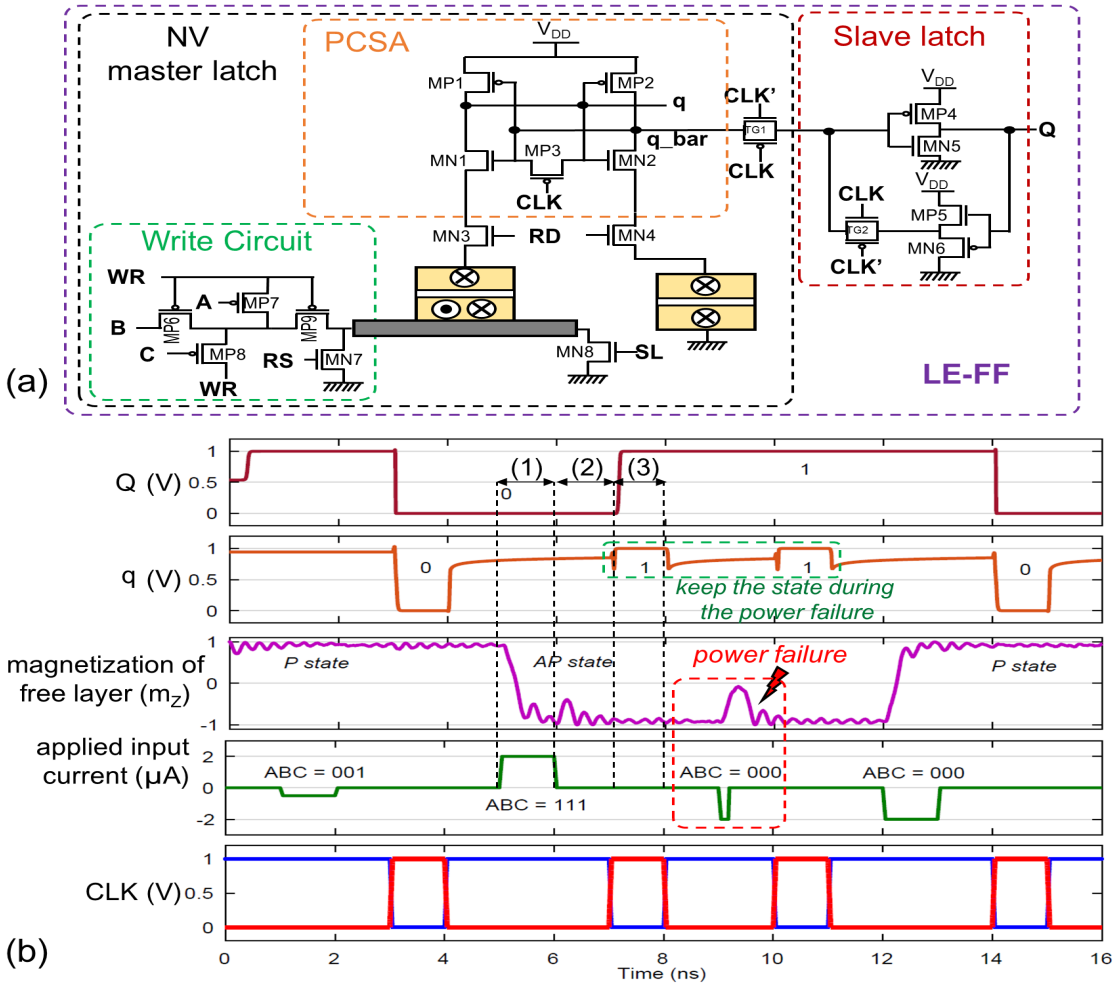


Figure 5.13: Circuit-level design of proposed 3-input SHE-based LE-FF, and (b) transient response for three different input ABC= "001", "111", and "000" in presence of power failure. Three different modes are shown: (1) store mode, (2) standby mode, and (3) sense mode.

Area Analysis

The gate counts and area performance of the ISCAS-89, ITC-99, and MCNC benchmarks with and without NV-Clustering are provided in Table 5.7 and Figure 5.14, respectively.

Table 5.7: NV-Clustering Gate Equivalent Reduction.

ISCAS 89	Circuit Function	Latch	Gate Equivalent		Improvement %
			Baseline	NV-Clustering	
s27	Logic	3	10	8	20
S298	PLD	8	119	49	59
S349	4-bit Multiplier	15	161	102	36
S400	TLC	21	164	144	12
S420	Fractional Multiplier	16	218	152	30
S526	TLC	21	193	83	57
S820	PLD	5	289	259	10
S838	Fractional Multiplier	32	446	329	26
S1196	Logic	18	529	459	13
S1423	Logic	74	657	396	40
S15850	Logic	534	9772	8942	8
S38584	Logic	1426	19253	12504	35
ITC-99					
b02	FSM recognizes BCD	4	22	15	32
b05	Elaborate the CM	34	861	718	17
b09	Serial-to-serial converter	28	129	100	22
b10	Voting system	17	155	124	20
b11	Scramble string	31	437	393	10
b12	Guess a sequence	121	904	761	16
b13	I/F to sensors	53	266	198	25
b14	Viper processor	245	4444	4112	8
MCNC					
bigkey	Key Encryption	221	2383	2172	9
clma	Bus Interface	33	5763	5314	8
dsip	Encryption Circuit	224	744	714	4
sbc	Bus Controller	28	490	417	15

Herein, all building blocks including functional and buffer components, except FFs, are counted as a gate-equivalent. Whereas no gates are clustered with an NV-FF realization, its number of gate-equivalents is identical to a CMOS-only realization. Meanwhile, NV-Clustering leverages MGs, which can implement one (or a set of) Boolean function (s). For instance, benchmark circuit s1423 has 657 gates, which is reduced to approximately 60% of the original number of gates, 396,

in the LE-FF implementation. This improvement leads to a reduction in area consumption and routing complexity. Figure 5.14 depicts the total area of benchmarks including the interconnection, combinational, and sequential components regarding these different implementations. As is mentioned above for combinational circuits, NV-FF and CMOS implementations occupy a similar area. However, from a sequential point of view, implementing NV-FFs and LE-FFs requires additional peripheral circuits such as write and read circuits, which can incur area overhead. Hence, the NV-FF implementation occupied the largest area among the implementations. On the other hand, a reduction in the equivalent gate count decreases the area of both combinational and interconnection components. Owing to the back-end process vertical integration of spintronic devices, the area of NV elements can be greatly reduced, hence LE-FF implementations indicate the least area consumption. As shown in Figure 5.14, the area overhead of ISCAS-89, ITC-99, and MCNC benchmarks using LE-FF average 15%, 10%, and 5%, respectively, area reduction over NV-FF realization.

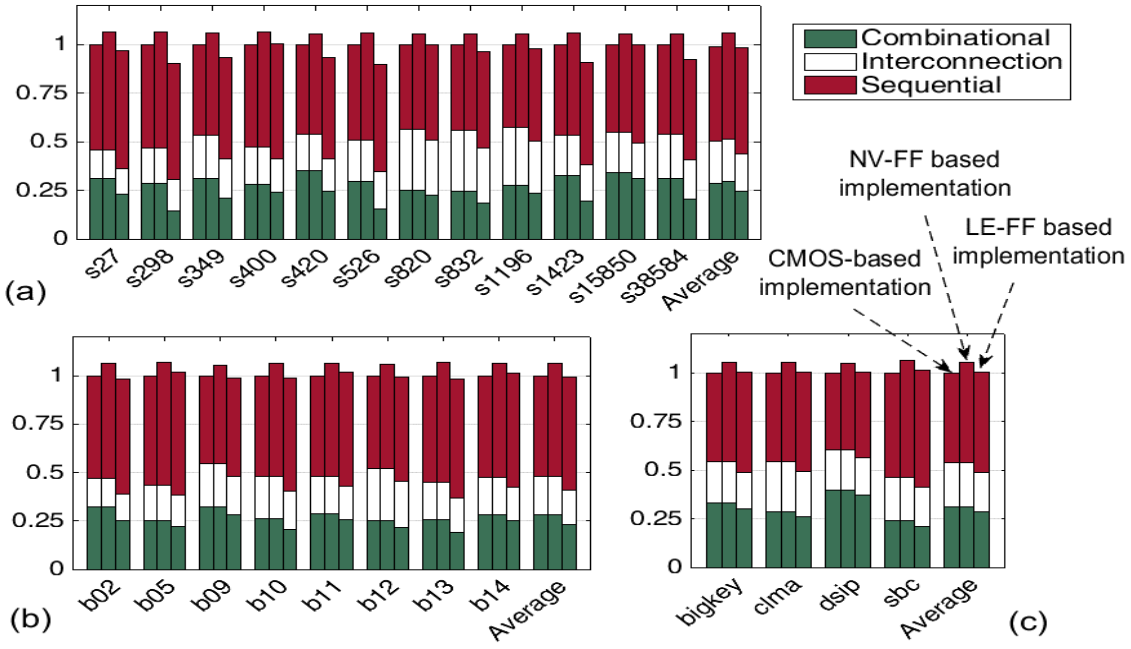


Figure 5.14: Normalized area consumption compared to CMOS-based implementations for different benchmarks.

Power Analysis

Herein, the power consumption of ISCAS-89, ITC-99, and MCNC benchmarks using NV-FF and LE-FF are analyzed. Figure 5.15 depicts the power consumption regarding the combinational blocks. Generally, our implementations depict a good amount of power reduction for all benchmarks. However, due to the constraints in implementing large logic functions using three and five input MGs, in some benchmarks such as *dsip*, the differences between the two implementations are insignificant. Although this issue can be readily addressed by developing larger MGs with a higher number of inputs, increasing the number of inputs also increases the complexity of the MG. Figure 5.15 depicts an average of 22%, 13%, and 5% power reduction using the NV-Clustering average for ISCAS-89, ITC-99, and MCNC benchmarks, respectively.

The total power dissipation for a few ISCAS-89 benchmark circuits including the interconnections, combinational, and sequential blocks are shown in Figure 5.16. Because NV elements within the sequential designs consume much more power than combinational circuits, the total power improvement of NV-Clustering over the previous NV implementations are reduced, especially in the designs with a larger number of FFs.

To address this issue, a *state checking block* can be designed within an FF. It is composed of four transistors, which compares the new input of an FF with the stored value in the NV element. If the values are equal, the applied input is neglected and no write operation is required. Hence, the number of write operations might be decreased. Because write power for Spintronics is much larger than power dissipation of the additional transistors, the overall power consumption will be reduced. Otherwise, if the values are different, the FF operates as previously described. It is worth noting that although the total power consumption might be decreased, the delay should remain unchanged to provide correct functionality. Moreover, because of this additional circuitry, new designs will occupy more area in comparison with the previous designs. Therefore, there is a

trade-off between power and area consumption.

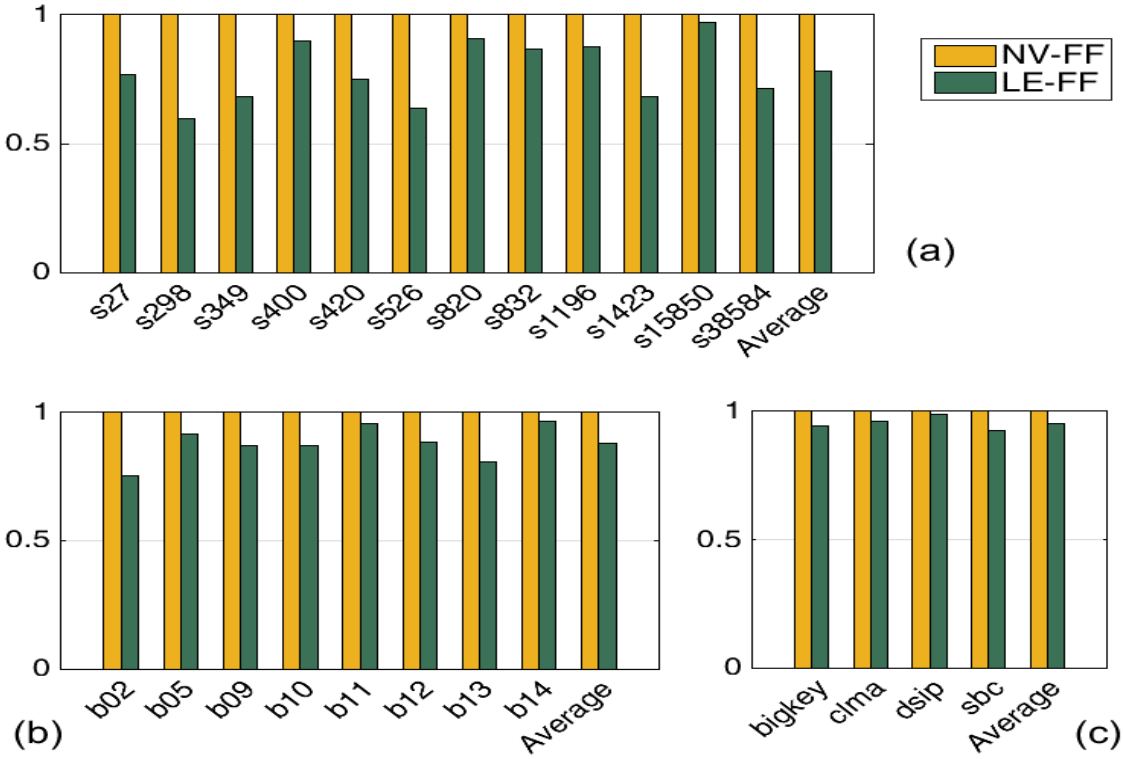


Figure 5.15: Normalized power dissipation compared to NV-FF. Results based on realization of combinational components.

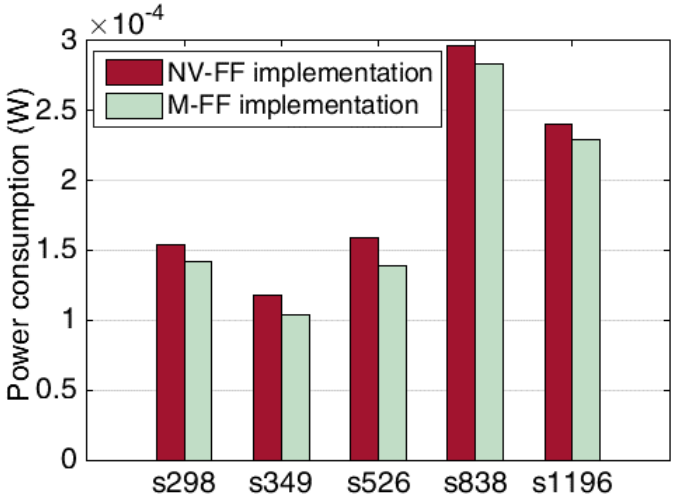


Figure 5.16: Total power consumption for selected ISCAS-89 circuits.

Delay Analysis

In this Section, the delay of LE-FF circuits with NV-FF implementations for different benchmark categories are compared. The optimized RTL Verilog HDL codes for the benchmarks are synthesized using a Synopsys Design Compiler, and then worst-case timing paths are obtained through applying STA on compiled netlists using Synopsys PrimeTime. The obtained results regarding benchmarks are shown in Figure 5.17. As it can be seen, the delay is directly proportional to the number of combinational components. It means that if the number of FFs is minimal and the number of replaced combinational blocks is maximum, then the delay is reduced to the greatest possible extent. It is worth noting, that the obtained results herein are at the gate level, and physical design parameters are not considered. As shown in Figure 5.17, the delay reduction for selected ISCAS-89, ITC-99, and MCNC benchmarks using NV-Clustering average 14%, 11%, and 4%, respectively, over NV-FF.

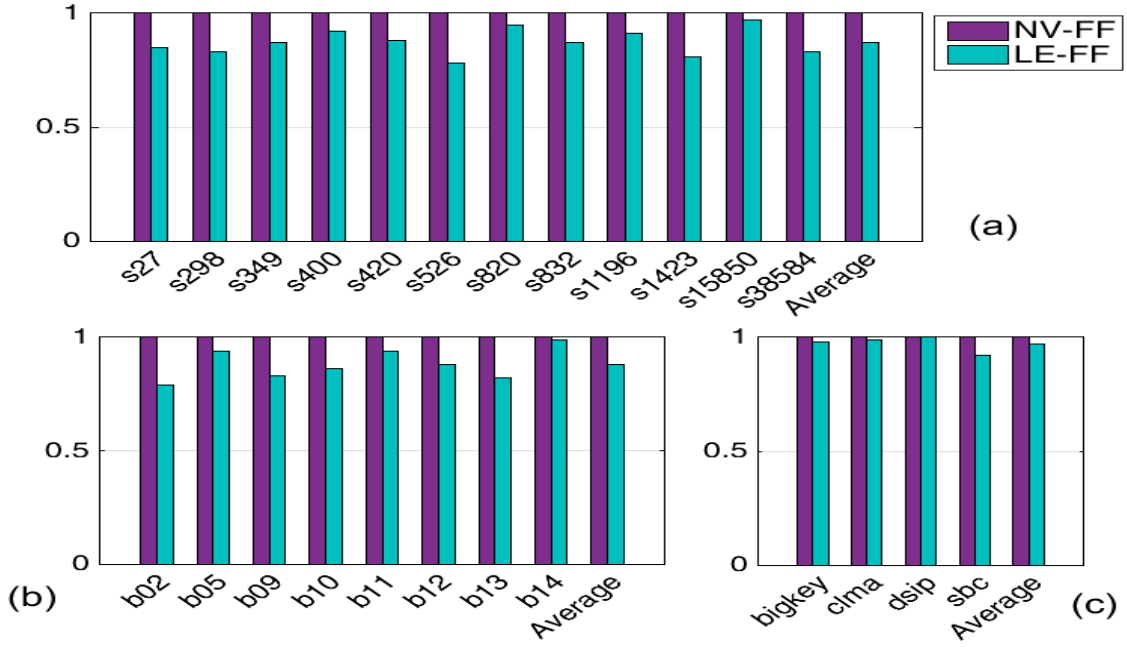


Figure 5.17: Normalized delay compared to NV-FF based implementations for different benchmarks.

Resumption Overhead

In energy harvesting systems, the power supply has a limited capacity. On one hand, in a CMOS-based design, if the system is powered down, then volatile memories lose data and up to a few milliseconds [137] is necessary to restore information after a new power-up. Furthermore, this charge/discharge cycle, which is an intrinsic characteristic of energy harvesting devices, may occur hundreds of times per second. It means the system might consume its entire power supply capacity to restore to the initial states. On the other hand, although NV-FF and LE-FF implementations provide power failure tolerant designs, the required power consumption of write operations for non-volatile elements remains an issue. Hence, due to the capacity limitation of power supplies in addition to the aforementioned issues, various conditions should be considered in order to choose between CMOS-based or NV-based implementations. Two of the main conditions are: (1) a total number of completed operations, and (2) power failure rate. According to the equality $ConstantPowerSupply = \sum_i^m n_i \times P_i$, where, m is the total number of operations, n is the number of operation i, and P is the required power consumption of operation i, in a low/free power failure situation, volatile CMOS-based implementations perform more operations than non-volatile based designs. However, in the environment with a high occurrence rate of power failure, the number of completed tasks for CMOS is excessively reduced, which degrades the overall system performance. Since the power supply capacity and power consumption of each operation are constant, the usage of an NV approach is affordable if the power failure rate is relatively high, which can disable CMOS-based designs functionalities.

Due to the abovementioned conditions, there are two potential scenarios to be considered. *Scenario #1* corresponds to the case when **intermittency is absent**, in which power failure did not occur during the processing interval under observation. *Scenario #2* represents the case in which **intermittency is present**. Considering *Scenario #1*, the application of MTJs in memory device

applications [138, 139], the retention time, $\tau = \tau_0 exp(\Delta/kT)$, is arranged to be 10-15 years by choosing a thermal barrier, Δ, between 40-60 kT. On the other hand, the critical spin-current is linearly proportional to the thermal barrier, Δ. Thus, for applications herein that do not require retention times of years, we investigate via simulation the reduction of the thermal barrier of nano-magnets by means of uniaxial anisotropy, in addition to other possibilities such as lowering their volume or their saturation magnetization. This ultimately reduces the charge currents that are required for write operation, which can result in significant energy improvement due to the quadratic relationship between the Ohmic (I^2R) losses and the input write currents. In this chapter, LE-FFs using SHE-MTJ devices with 30kT energy barriers are investigated that can achieve retention times ranging from minutes to hours, while providing at least 50% energy reduction.

Figure 5.18 shows the power-delay-product (PDP) values for the two scenarios. In the intermittency-absent condition, the obtained PDP results for CMOS-based designs are relatively lower than the other implementations because of the high speed/low power switching of CMOS. Whereas in the intermittency-present scenario for various ISCAS-89, ITC-99, and MCNC benchmark circuits, the results exhibit an average of 14%, 12%, and 4% PDP improvements, respectively, for LE-FF (Δ= 40kT) based designs compared to NV-FF based implementations. Further PDP improvements can be achieved by using low energy barrier SHE-MTJ devices (Δ= 30kT) within LE-FFs at the cost of smaller retention times. However, in the energy-harvesting-powered IoT devices, retention time in the range of days and hours could be sufficient to achieve proper functionality. Thus, leveraging SHE-MTJ devices with 30kT energy barrier in intermittency occurred situations, provides up to 12%, 48% and 39% average PDP improvements compared to CMOS-based designs, NV-FF based designs, and LE-FF based implementations with SHE-MTJ devices having Δ= 40kT, respectively, without incurring any area overhead. It is worth noting, that the results provided herein are obtained at the gate level and physical design parameters are not considered within the document space available.

Algorithm 3 NV-Clustering Methodology

```
1: procedure MAIN()
2:     Input: Hardware Description Language (HDL) code
3:     Output: optimized HDL code
4:     find all FFs and update FF_list
5:     for FF in FF_list do
6:         if size (create_cone (FF)) ¿ 1 then
7:             replace cone_gates by MG_FF
8:         else
9:             replace cone_gates by NV_FF
10:        end if
11:        update HDL code
12:    end for
13: end procedure
14: procedure CREATE_CONE()
15:    Input: a combinational gate, i.e. G
16:    Output: list of gates connected to a FF, i.e. cone_gates
17:    input_list = find_input (G)                    ▷ return list of G's input
18:    for item in input_list do
19:        if criterion #3 or criterion #4 is violated then
20:            input_list.remove (item)
21:        end if
22:    end for
23:    for item in input_list do
24:        tmp_gate = find_gate (item)                ▷ return gate with item as its input
25:        cone_gates.append (tmp_gate)
26:        if check (cone_gates) then
27:            create_cone (tmp_gate)
28:        else
29:            cone_gates.remove (tmp_gate)
30:        end if
31:    end for
32:    return cone_gates
33: end procedure
34: procedure CHECK()
35:    Input: cone of gates
36:    Output: Boolean expression
37:    if criterion #1 or criterion #2 is violated then
38:        return FALSE
39:    end if
40:    return TRUE
41: end procedure
```

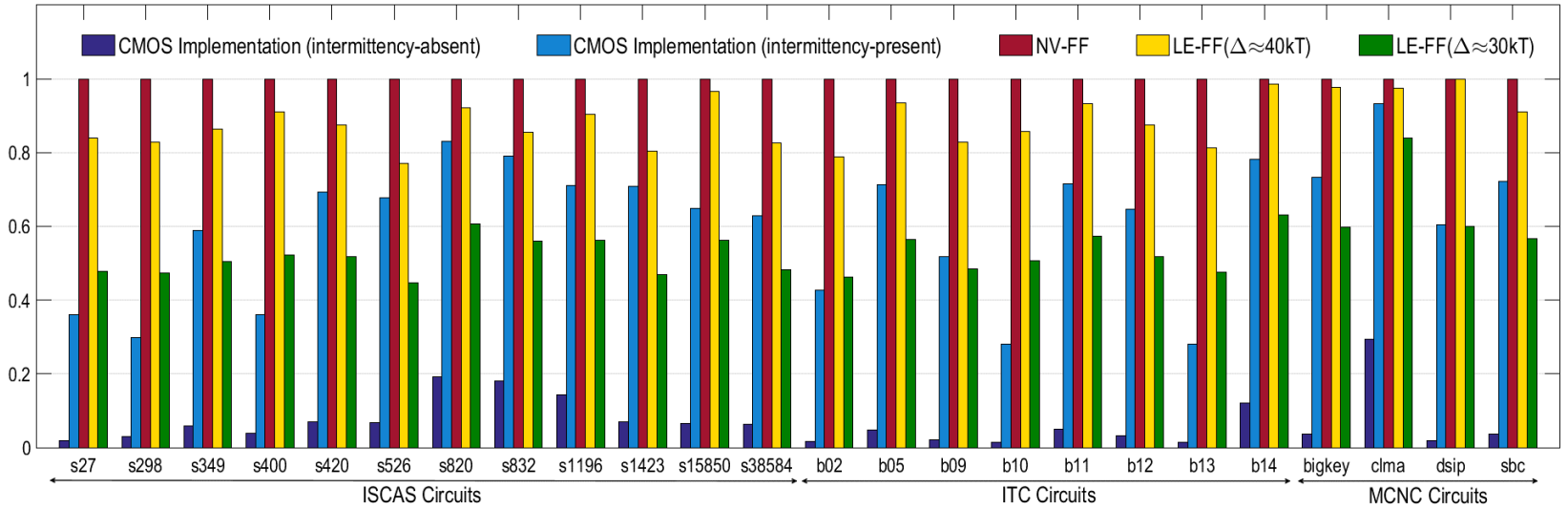


Figure 5.18: Normalized PDP compared to NV-FF based implementations for *intermittency-absent* and *intermittency-present* scenarios.

CHAPTER 6: SECURE INTERMITTENT-ROBUST POLYMORPHIC GATE-BASED DESIGN

Secure Intermittent-Robust Computation for IoT Devices

Advancing beyond previous intermittent processors that utilize non-volatile memory (NVM) resources, which are distinct from the processing datapath, we propose the SIRC computing architecture based on spintronic devices leveraging their inherent non-volatility within the logic datapath itself, while avoiding the energy overhead of intermittent check-pointing, routine data exchange between tasks, and datapath pipeline registers. Thus, the intermittent operation can be intrinsically supported without the burden of additional circuitry or software-based task decomposition. In the case of unpredictable power interruption, the instantaneous condition of all processor internal states will remain within its own datapath without the need to reload all the previous operands to help mitigate power charging and spoofing vulnerabilities.

One promising beyond CMOS technology, which has non-volatility, is Spintronics. Moreover, the unifying computational mechanism underlying all of the Magnetic Tunnel Junction (MTJ)-based devices is the accumulation-mode operation that enables the realization of Polymorphic Gates (PG) as basic computational building blocks. PGs provide a functionally-complete set of Boolean logic expressions due to their intra-gate control, and can realize intermittent robust circuits that are the fundamental building blocks of the SIRC architecture. Figure 6.1(a) depicts the SIRC architecture at the system block level. It consists of a pool of NV-PGs, which are connected to input, output, and control signals, as well as sensitive NVM (low energy barrier), and NVM containing the encrypted nodes information. In Figure 6.1(b), SIRC operates as a 2-bit NV Full Adder (NV-FA), whereas, Figure 6.1(c) illustrates a 2-bit NV Multiplier (NV-M) by only adjusting control signals, which alter

the PGs' functions without any additional device overhead within the computational unit. NV-PGs can be cascaded to realize conjunctive or disjunctive Boolean gate realizations. By affixing one (or two) of the three (or five) input signals to ON or OFF states on demand during the circuit operation, then a 2(or 3)-input OR gate or a 2(or 3)-input AND gate can be realized, respectively. Both 3 and 5input NV-PGs are implemented and validated by SPICE circuit simulations using our model developed in [140, 141].

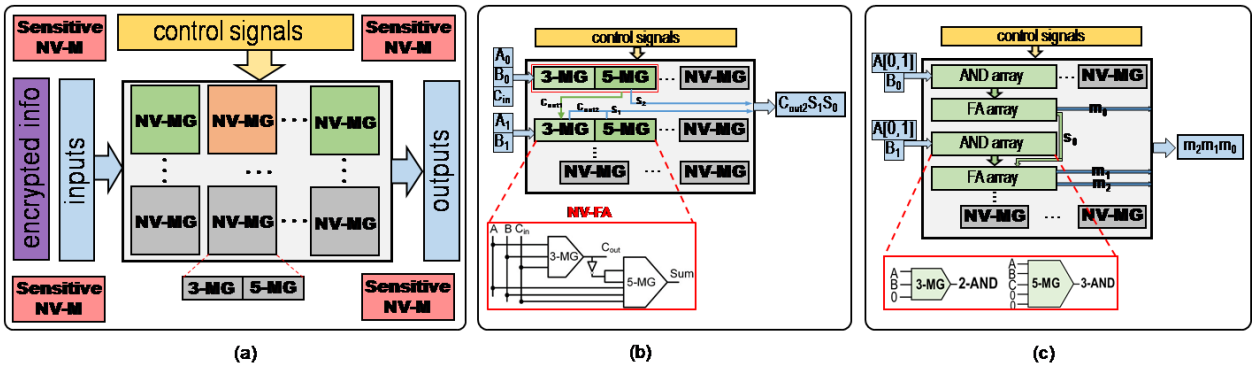


Figure 6.1: (a) SIRC computation pool of NV-MGs, (b) NV-FA arrangement using 3-MG and 5-MG, and (c) 2-bit NVM multiplier.

Vulnerabilities under Charging Attacks

In energy-harvested IoT devices, one of the most significant classes of attacks is a charging attack [142]. In wireless power transfer networks, it is assumed that several mobile and fixed Power Transmitters (PTs) and SIRC-embedded devices, which are considered as Power Receivers (PRs), communicate with each other. The attacker's goal is to decrease the efficiency of PTs, which results in the degradation or interruption of the system functionality. In general, a power transfer channel has some significant attributes that differ from a data communication channel. Therefore, possible

attacks against the SIRC architecture can be partitioned into two sub-categories: energy attacks and data (information) attacks.

a) *Energy Attack*: There are two potential scenarios to be considered. Scenario One: malicious PR nodes generate unnecessary energy requests and send false responses and feedback to the PT node (global power source), which results in decreasing efficiency of the overall power of a non-ambient source. In such environments, the malicious receiver nodes send charging requests in a compressed period, which cause other viable nodes to receive reduced or insufficient power for their store/computation operations. In this scenario, the attacker counterfeits its energy state. Scenario Two: a malicious PR node counterfeits or feigns the role of a PT. It emits radio frequency waves with the same frequency as the PT, but with different phase. Hence, the energy harvesting at the victim PRs could potentially be modified, or the attacker forms a cooperative relationship with victim PRs.

b) *Data Attack*: A plethora of data attacks have been identified in the literature [143, 144]. Herein, the scope of data attacks focuses on those relating to power information. A common power-related information attack is a spoofing attack. In wireless power transfer networks, different types of energy-related data such as energy state, energy outage, signature, etc. will be broadcasted between PRs and PTs. In this scenario, an attacker (malicious node) can eavesdrop on the data of the other PRs or even PTs and utilize the captured information to decrease and/or collapse throughput of the network. In this case, three possible scenarios might occur: (1) if a malicious node (attacker) knows its adjacent PR (victim) will deplete its energy at the time T, it can broadcast energy requests at time t$<$T, to prevent the victim from receiving energy, thus precipitating its interruption; (2) the attacker can change its or the victim's device identity in a way that the victim could not receive energy. It also can feign as a PT to adjacent PRs and store their energy requests without any response; and, (3) the attacker can broadcast fake responses to the received energy from PTs, in particular, the attacker demands additional energy whereas it has sufficient energy.

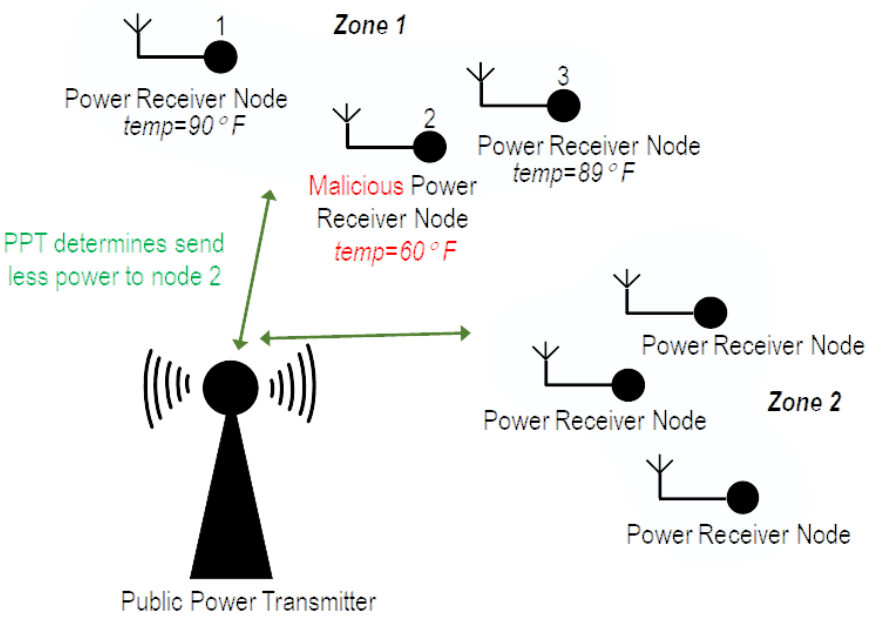


Figure 6.2: Feasible countermeasure for charging attack by marking a possible malicious node.

SIRC Mitigation of Charging Attacks[1]

All PTs and PRs are equipped with NV memories to store encrypted data. This data can be fixed, such as the average power consumption for a specific duration at design time, or can be changeable, such as the remaining power, number of received/sent requests, and number of zones at runtime. Power transmission process can be performed using both omnidirectional or directional antennas. (1) The PT propagates RF power via omnidirectional antennas: every PR inside a specific zone starts charging, simultaneously. Meanwhile, the malicious nodes' lives can be extended if they can power off and power on repeatedly, to extend their effect on the entire system. Hence, when a PT receives information and stores it within its NV memory from several PRs in the same zone, it then checks their correctness/incorrectness using a majority voter, as shown in Figure 6.2 For

[1]©2018 IEEE. Reprinted, with permission, from [145].

instance, if node a1 in Zone A, reports information very different from the other nodes ($a_2, a_3, ...$) in Zone A, the PT updates NVM and marks a1 as a potential attacker, which receives less power than previously provided until it functions similarly to the other nodes. (2) The PT propagates RF signals using directional antennas: malicious nodes moderately send energy requests to halt other PRs' functionalities. In this case, based on the stored data for each PR node at design time, including approximate power consumption, the PT can determine they are issuing either plausible or unreasonable requests. If a PR shows suspicious behavior, then the PT can penalize it or even modify power transmission parameters so that it receives less energy to preclude the malicious node.

Cryptographic methods can be implemented using both software algorithms and hardware elements. Although the former class is more flexible, the latter one can be significantly more energy-efficient, tailored to the need, and bloat-free, which can make it much more suitable for energy-harvested IoTs. In cryptography, one of the most dangerous and ubiquitous attacks is the side-channel attack, which herein is a power analysis attack (PAA). An adversary can use PAAs to capture different aspects of power supply when the crypt-decrypt process is performed to break the cryptographic algorithm. Our efficient PAA countermeasure is based on the design presented in [144] with the following differences: (1) there are no registers required within datapath; (2) we can reprogram one block to operate with the different functional blocks in different situations at both design time and runtime; (3) a selection operation is performed by using only one selective transistor, which connects appropriate element's output to the final output via sense amplifier; and (4) the random noise insertion process is performed using spin-based low power and high efficiency true random number generator (TRNG). Figure 6.3, depicts possible power analysis countermeasure utilizing power masking method. The role of the randomized selector (RS), which includes selector and TRNG, is to activate each of functional block (FB) based on the portion of inputs. Due to the random behavior of RS, the total power consumption of this module will vary randomly, which

assists the goal of masking the power consumption.

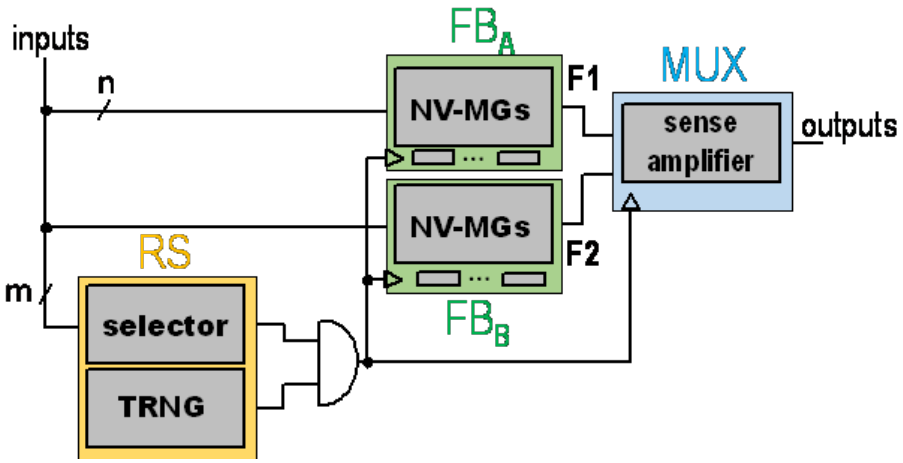


Figure 6.3: Power masking countermeasure for possible power analysis attack. F1 and F2 perform the same function with different power consumption.

Although a general way to make a design resilient to power failure is that all FF should be replaced by NV-FFs [32], in our approach which leverages NV-PGs, non-volatile elements are also able to realize logic operations while storing values. Therefore, a cone (sequence) of gates with only one fan-out connected to a flip-flop can be implemented using one (more) PG-FF(s). This enables reconfiguration of the design to implement a function with different structures, which results in different power profiles. Hence, this technique can be utilized within the power-masked cryptosystem implementations. To exemplify the functionality of this method, the `s27` circuit from the ISCAS89 benchmark suite is selected as a proof-of-concept, as shown in Figure 6.4. First, a cone of gates including the FF is selected, which is shown with red dashed lines. Then, this selection is implemented using two PG-FFs and five selector circuits. As depicted in Figure 6.4, the implemented design can be reconfigured using two reprogramming random bits, K_1K_2, in order to produce all equivalent implementations. The portion of the design which can be reconfigured

through K_1 and K_2 bitstream are: 1) select input or its inverted (input_bar) signal, 2) determine PGs functionalities, and 3) drive out or out_bar to the output pin. Figure 6.4 depicts all four possible designs with similar functionality. For instance, if generated keys are K_1K_2 = "00", first $\overline{A}, \overline{B}$, and K_1 are connected as inputs to the first PG-FF, which functions as a 2-input AND gate (K_1=0). Then K_1K_2 signal is XORed and selects out_bar and pass it to the second PG-FF. Its other inputs are C and K_2. Due to the produced connection using K_1K_2 = "00", the equivalent behavior of the design is $(\overline{\overline{A}.\overline{B}}).C$. This methodology can be leveraged for all cone gates connected to FFs to convert them to power maskable units with the intermittence resiliency feature.

Herein, the SHE-MTJ model developed in [107] is utilized to design a 3-input PG. The functionality of the SHE-PG based designs are verified by SPICE circuit simulation. Table 6.1 summarizes power consumption results for four different implementations regarding generated keys. For instance, the design produced by keys, K_1K_2 = "11", which is equivalent to D4 circuit in Figure 6.4 has the highest average power consumption for all possible input combinations. The reason is that because PG-FFs function as 2-input OR gates, which leads to a higher number of ON transistors, which pass a higher input current and thus incur a higher power dissipation. If after generating K_1K_2, the keys remain fixed during operating for all possible 3-input combinations, eight distinct possible power traces produced. Whereas, keys can have four different values, which result in 32 different combinations of power traces, which are shown in Figure 6.5. Based on our approach, the generalized equation for calculating all required power traces is expressed by $2^m \times 2^n$, where m is the number of key bits and n is the number of input bits. Therefore, by extending this method for all possible cone gates, more number of power traces are required by the attacker to extract the private key using differential power analysis attacks.

As mentioned above, the conventional power-maskable approaches include two separate units, in which their inputs are latched by registers and function similarly with different power cost [144]. This results in an area overhead almost twice as large as the original design, in addition to the

limited variety in power-managed units for masking power. Both contribute significant drawbacks of conventional power masking methods. Whereas, the proposed SIRC architecture leverages non-volatile SHE-based PG-FFs, a power-obscured area-dense energy-aware intermittent PAA resilient design is obtained. It realizes increased side channel immunity for IoT due to the PGs capability to transform between AND, OR, etc. gates at runtime.

Table 6.1: Generated Keys and Their Corresponding Average Power Consumption.

k_1k_2	Inputs	Functionality		Equivalent Design in Fig. 6.4	Average Power Consumption (μW)
		MG1	MG2		
00	A'B'C	NAND	AND	D1	68.6
01	A'B'C'	AND	NOR	D2	101.5
10	ABC	OR	AND	D3	98.8
11	ABC'	NOR	NOR	D4	131.7

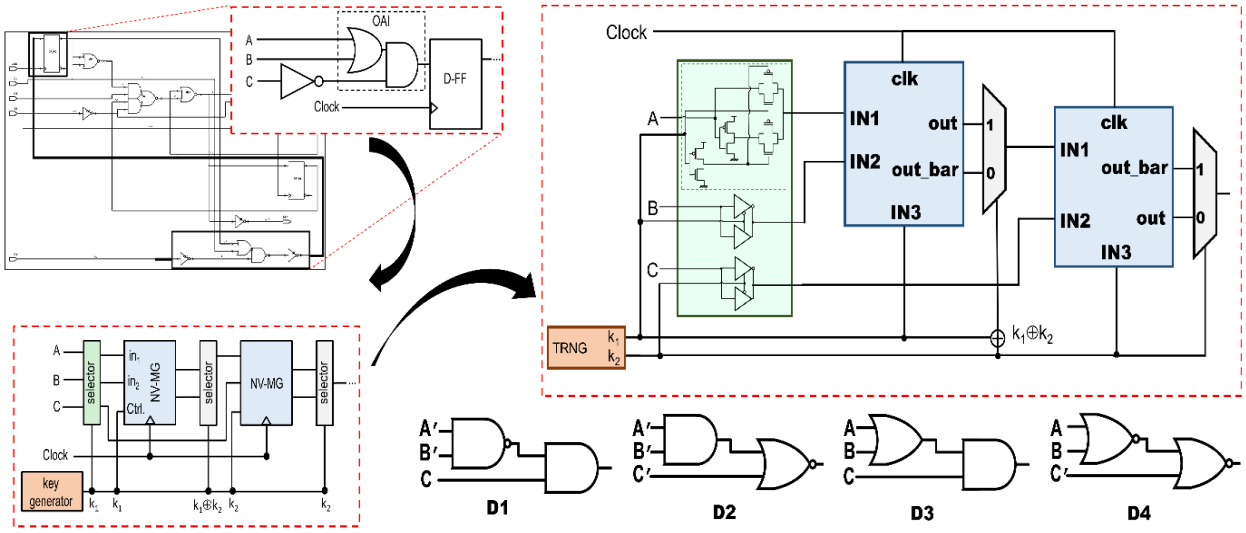


Figure 6.4: `s27` schematic (top left), selected cone gate (bottom left), developed MG-FF based design (top right), and equivalent logic realizations (bottom right).

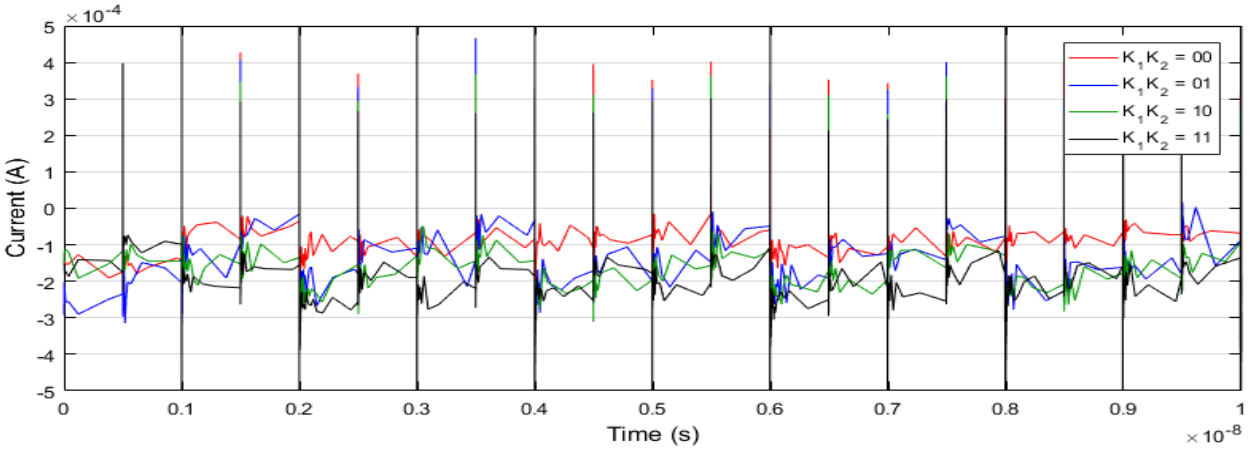


Figure 6.5: Power traces results for all possible K_1K_2 combinations.

Logic-Encrypted Synthesis for Spintronic-Embedded Datapath Design

Secure intermittent-robust PG-based design[2]

Polymorphic electronics were introduced in [147], whereby a PG would be an AND gate or OR gate depending if VDD is 3.3V or 1.5V, respectively. Various CMOS-based polymorphic gates have employed mechanisms such as gradations in VDD and signaling levels, or temperature to achieve reconfigurability. Meanwhile, the spin-based devices can naturally function as polymorphic threshold gates since their computational mechanism is an accumulation-mode operation that realizes reconfigurable logic functions with inherent security attributes [123]. Figure 6.6(a) shows the schematic of 3-input Non- Volatile Polymorphic Gates (NV-PGs), which is designed using spin- Hall Effect (SHE)-based Magnetic Tunnel Junction (MTJ) devices. A pre-charge sense amplifier (PCSA) [136] is utilized to sense the state of the SHE-MTJs. Reference MTJ dimensions are designed such that its resistance value in the parallel configuration is between low resistance, R_{Low}, and high resistance, R_{High}, of the PG cells. The minimum current required for switching the

[2]©2018 IEEE. Reprinted, with permission, from [146].

state of the SHE- MTJ devices is called the critical current (IC), which is relative to the dimensions of the device. In an n-input NV-PG, the device is designed such that at least (n-1)/2 of the input transistors should be ON to produce a switching current amplitude greater than the critical current. For instance, by affixing one of the three input transistors in ON or OFF states upon demand during the circuit operation, then a 2-input OR gate or a 2-input AND gate can be realized, respectively.

The functionality of the proposed 2-input OR, NOR, AND, and NAND gates implemented by SHE-MTJ based PGs have been validated by SPICE circuit simulator using parameters listed in Table 6.1, as shown in Figure 6.6(b). Figure 6.6(c) shows the proposed 3-input and 5-input PGs containing two and three control bits, respectively, which can determine the functional modes of the gates. For instance, various functional modes of a 5-input PG are shown in Figure 6.6(d). The PGs utilize intra-gate control to provide a functionally-complete set of Boolean logic expressions. Although the PG-FF circuit is similar to LE-FF design, in PG-FF the master latch is NV-PG.

Secure PG-FF design

The reconfigurability characteristic of SHE-MTJ based PGs is achieved by means of the multiplexer (MUX) and control bits existing in their structures. Despite the area and performance overheads imposed to the design by using PGs, they can be utilized for logic encryption in addition to enabling intermittent computing, which can provide the hardware with increased security capabilities. In the proposed approach, each PG and its corresponding MUX can be leveraged as the encryption key gates, which increases the key bit space. It means to retain the correct operation of the design, the appropriate key bits of both PGs and MUXs should be applied. The length of the key is determined by the number of inserted PG-FFs, which is normally greater than or equal to the number of output bits. While, in the previous MUX- based logic encryption methods [148, 149], the key length is limited to the number of outputs in a design. The vulnerability of PG-FF based

circuits is similar to that of the designs that are secured by the random insertion of XOR/XNOR gates [148, 150]. In the proposed approach, the PGs will be inserted to the logic circuits based on a methodology that is designed to enable intermittent computing. Therefore, the main focus of the methodology is on intermittency- resilient and the logic encryption is the secondary objective. Thus, the inserted PGs and MUXs may not enable the intermittent-robust design to achieve the optimum Hamming distance (HD) of $\sim 50\%$, which is a security metric defined based on the number of bit positions at which a correct and faulty output are different. In order to minimize the memory overhead, the configuration bits of PGs and MUXs, which are considered as key bits should be stored in external non-volatile memory. To implement and synthesize an optimized, secure, and intermittent-resilient logic circuit using PG-FFs, a systematic methodology is developed that is described in the next section.

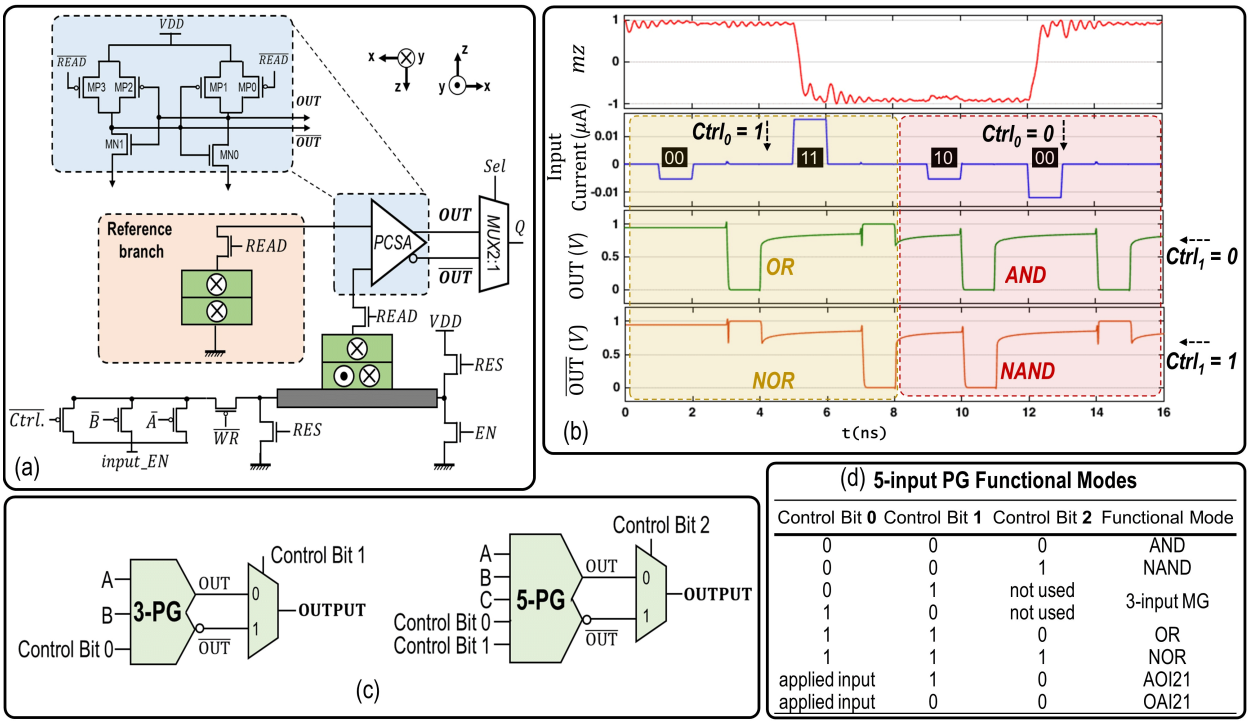


Figure 6.6: (a) SH-MTJ based 3-input PG, (b) 2-input OR, NOR, AND and NAND logic using 3-input PG, (c) 3-input and 5- input SHE-MTJ based PGs, (d) 5-input PG Functional Modes.

PG insertion methodology

To design optimized NV architectures using the proposed PG-FF, we develop a methodology that incorporates all PG-FF features to design partially-secure power-failure tolerant architectures. This approach leverages the maximum capability of PG-FFs in terms of replacement and implementation steps, which incorporates various criteria to design a tolerant circuit in the presence of power failure with minimum PDP overhead.

The proposed algorithm, which is developed in Python consists of two main procedures: (1) **`intermittency()`**, and (2) **`logic encryption()`**. The PG insertion methodology takes a Hardware Description Language (HDL) representation of a datapath and PG- based gate modules as its inputs and produces an optimized NV-enhanced datapath. The proposed methodology is described in Algorithm 4, which first explores the HDL of the logic circuit and finds the gates and pipeline registers that can be combined and replaced by spin-based PG-FF circuits, and the remainder of the pipeline registers will be replaced by NV-FFs. Next, the optimized intermittent-robust design is investigated to encrypt the datapath and generate a key based on Hamming distance (HD) calculations as a security metric. In particular, the algorithm first finds all of the FFs in the design, and then checks the cone of logic gates connected to the inputs of the FFs. If each cone of gates meets the circuit-level criteria mentioned below, then the cone and its corresponding FF can be replaced by a PG-FF cell. The three primary criteria regarding the intermittency issue are:

Criterion #1: it should be possible to implement the cone of gates with a single PG. Since each PG-FF operates in one clock cycle, the cone of combinational logic gates that are merged with a master latch should operate within one clock cycle to ensure the correct functionality. Hence, the use of more than one PGs for complex functions could increase propagation delay, which might lead to timing violations.

Criterion #2: fan-out of every gate in the cone should not exceed one. This is mainly because in the process of PG-insertion multiple logic gates can be implemented by a single PG that exists in the structure of the PG-FF's master latch. Therefore, the logic gates existing in the cone will not have separate outputs to drive other logic gates, and there will be only one output for the PG showing the combined logic of the merged gates.

Criterion #3: none of the gates in the cone should be connected to the output of another FF. This will cause the selected cone to include two FFs requiring two clock cycles for operation, while based on the developed algorithm the cone will be replaced by a single PG-FF resulting in a timing violation. Therefore, due to the timing considerations, each of the cones can include only a single FF and multiple logic gates.

If all of the aforementioned conditions are satisfied, then the cone of gates and their corresponding FF will be replaced by a single PG-FF. Otherwise, only the FF is replaced by a simple NV- FF. Herein, the primary objective of the algorithm is an implementation of intermittent-robust datapaths. The secondary objective is enhancing hardware security through logic encryption using the inserted PGs. In order to reduce the overhead of logic encryption, the proposed algorithm follows a recursive process to find the minimum key length required to achieve the desired security, which is directly related to the number of inserted PGs utilized for encryption. In particular, first, the logic-encryption procedure takes the intermittent-resilient datapath from the intermittency procedure and starts with using only one PG to generate the key and calculates the HD between the correct and wrong output bits. Then, the procedure checks the below criteria (4) and (5), and if they are achieved it will stop. Otherwise, it will increment the number of PGs utilized for producing the key and repeats this process until one of the below criteria are met:

Criterion #4: roughly 50% HD is achieved. To maximize the security of a PG-inserted design, the correlation between the wrong output and the correct output should be minimized to achieve

better encryption. Thus, the measured HD value needs to be approximately 50% to demonstrate a highly-encrypted implementation.

Criterion #5: increasing the key length has less than 1% effect on the calculated HD values. This means that if increasing the number of PGs used for logic-encryption is not significantly improving the HD values, then the procedure stops and outputs the key. In particular, every time that the key length is incremented, the following expression $HD_{(n)} \approx \frac{1}{m}\sum_{i=n-m-1}^{n-1} HD\_list[i]$ is used to compare the current HD value with the average of the last m measured HDs, where m is defined by the user based on the security demands, and n is the total number of inserted 3- and 5- input PG-FFs. Finally, the key bits that satisfy the security metrics with the minimum overhead, are stored in an external NVM, and the encrypted intermittent-resilient datapath is generated.

Simulation Results

In this section, we have utilized ISCAS-89, ITC-99, and MCNC benchmark circuits to evaluate the performance of our proposed PG-insertion methodology. For instance, the third row in Table 6.2 lists the gate counts of various ISCAS-89 benchmark circuits when the FFs are simply replaced by NV-FF, while the fourth row shows the decreased number of logic gates when the PG-insertion methodology is applied. Moreover, the last three columns illustrate the investigated security metrics including key length, HD, and logic key that is the maximum number of PG-FFs used within the datapath. The key length is directly proportional to the number of 3- input and 5-input PGs inserted into the design. The best HD values are achieved when all of the PG-FFs are considered as logic keys.

However, in larger designs, the obtained HD values are relatively low since the ratio of inserted PGs to the total number of gates existing in the design is small. This is mainly because the primary goal of the proposed PG-insertion methodology is to support intermittent- computing, while various

alternative methods proposed in [148, 151] can be leveraged to further fortify the security of the design.

Algorithm 4 PG-insertion Methodology

Input: Hardware Description Language (HDL) code
Output: Logic-encrypted intermittent-robust HDL code
procedure `INTERMITTENCY()`
    gate_list ← all FFs in a netlist
    for i ← 1 to length(*gate_list*) **do**
        input_list ← inputs of connected gate to $gate_i$
        for item in *input_list* **do**
            check (criterion #3)
            update (*input_list*)
            check (criterion #1 and criterion #2)
            update (*gates_cone*)
            go to 6 until one of each criterion is violated.
        end for
        replace (*gates_cone* by PG_FF) **if** size (*gates_cone*) ¿ 2 **else replace** (*gates_cone* by NV_FF)
        update HDL code
    end for
end procedure
procedure `LOGIC ENCRYPTION()`
    for n ← 1 to #inserted PG-FFs **do**
        key_size ← $2^{3n_1+2n_2}$ ▷ n ← n_1(#5-PG-FFs) + n_2(#3-PG-FFs)
        compute $HD_{(n)}$ based on *key_size*
        store (key bits in NVM) **if** (criterion #4 or criterion #5) **else** (HD_list ← $HD_{(n)}$)
    end for
end procedure

Area Analysis

Figure 6.7 compares the area consumption between CMOS, NV-FF, and PG-FF based implementations using various ISCAS-89, ITC- 99, and MCNC benchmarks. The results obtained are normalized to the area consumption of conventional CMOS-based circuits.

Table 6.2: PG-insertion results for ISCAS benchmarks.

ISCAS 89	**Circuit Function**	**Gate-Equivalent**		#Logic Key	#Key bits	Best HD
		NV-FF	PG-FF			
s27	Logic	10	8	2	4	0.142
s298	PLD	119	49	11	24	0.125
s349	4-bit Mult.	161	102	7	14	0.063
s400	TLC	164	144	22	49	0.229
s420	Frac. Mult.	218	152	6	12	0.057
s526	TLC	193	83	22	50	0.196
s820	PLD	289	259	10	20	0.035
s838	Frac. Mult.	446	329	14	28	0.061
s1196	Logic	529	459	8	20	0.015
s1423	Logic	657	396	54	116	0.135
s15850	Logic	9772	8942	207	423*	0.092
s38584	Logic	19253	12504	303	675*	0.037

*Using 128-length key bit, obtains 0.028 and 0.007 HD, respectively.

In all of the investigated designs, the interconnection area remains relatively unchanged, since replacing FFs does not significantly affect the interconnection circuitry. In the NV-FF based design, the combinational logic remains unchanged compared to CMOS-based design, while the area of the sequential logic is increased since the NV-FF includes more transistors in their structure than CMOS-based FF circuit due to the additional write and read circuitry. The proposed PG-insertion methodology leverages PGs to implement portions of the combinational logic within the PG-FFs without adding overhead to the sequential logic. Thus, the combinational logic in PG-FF based datapaths is smaller than CMOS and NV-FF based designs. For instance, benchmark circuit s1423 originally has 657 gates, which is reduced to approximately 60% of the original number of gates, i.e. 396 gates, after the PG-insertion algorithm is applied. This improvement leads to a reduction in area consumption, as well as routing complexity. Since the spintronic devices can be vertically fabricated on top of CMOS transistors, their corresponding area overhead is negligible. The results in Figure 6.7 exhibit that the proposed PG-insertion methodology can achieve an average of 7.1%,

4.2%, and 3.4% improvements in terms of area consumption for ISCAS-89, ITC-99, and MCNC benchmark circuits, respectively, compared to NV-FF based implementations.

Power-Delay Analysis

Figure 6.8 shows the power-delay-product (PDP) values for NV-FF, PG-FF, and low-energy barrier PG-FF based implementations using various ISCAS-89, ITC-99, and MCNC benchmark circuits. The results exhibit an average of 13.6%, 12.3%, and 3.5% PDP improvements, respectively, for PG-FF based designs compared to NV-FF based implementations, in which the CMOS-based FFs are simply replaced by NV-FFs. This improvement is mainly achieved through reducing the combinational logic in the PG-inserted designs as explained in the previous section, while the PDP values for interconnection and sequential logic remain unchanged. As shown in Figure 6.8, further PDP improvements can be achieved by using low energy barrier SHE-MTJ devices within PG-FFs at the cost of smaller retention times. However, in the energy-harvesting-powered IoT devices, retention time in the range of days and hours could be sufficient to achieve proper functionality. Therefore, the energy barrier of SHE-MTJ devices can be reduced to 30kT, realizing 25% reduction in switching critical current ($I_C \propto \Delta$) and approximately 44% decrease in write energy consumption ($E \propto I^2$), while providing non-volatility for a few hours. Thus, leveraging SHE-MTJ devices with 30kT energy barrier provides up to 48.5% and 40.5% average PDP improvements compared to NV-FF based designs and PG-FF based implementations with SHE-MTJ devices having $\Delta = 40kT$, respectively, without incurring any area overhead. It is worth noting, that the results provided herein are obtained at the gate level and physical design parameters are not considered within the document space available.

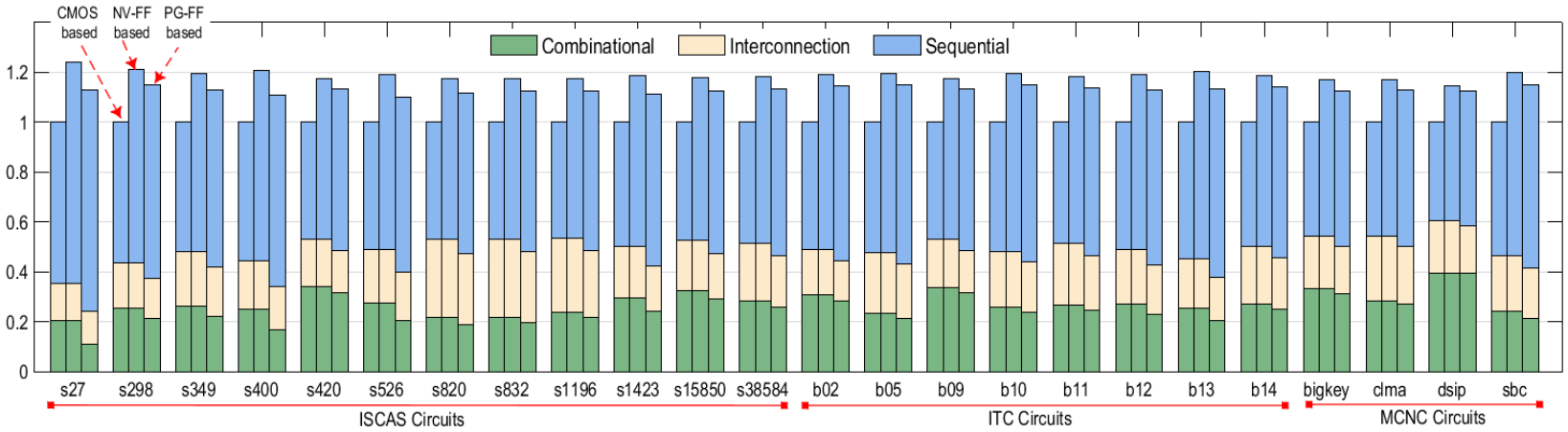


Figure 6.7: Normalized area consumption compared to CMOS-based implementations for ISCAS, ITC, and MCNC benchmarks.

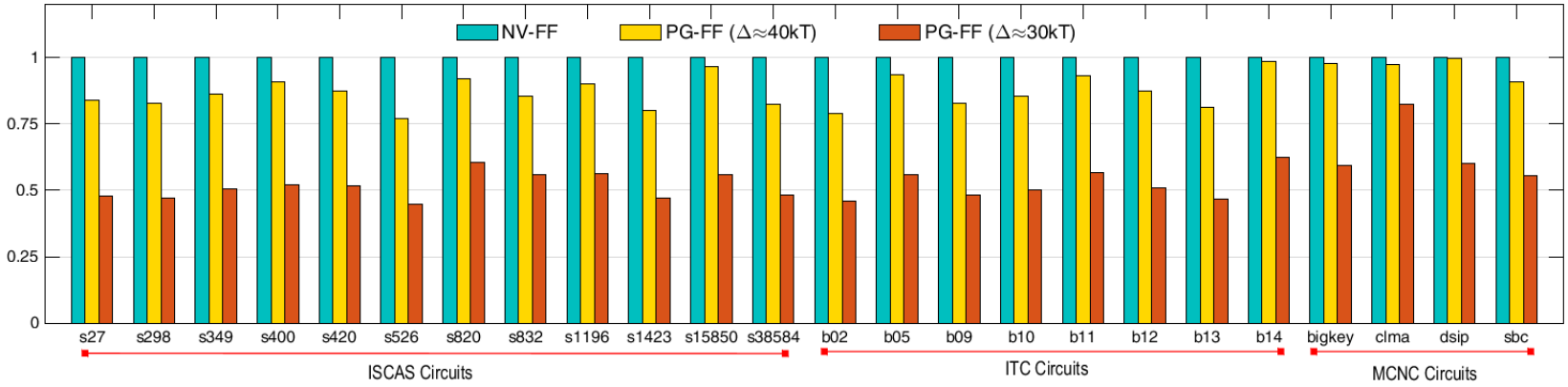


Figure 6.8: Normalized PDP compared to NV-FF based implementations for ISCAS, ITC, and MCNC benchmarks.

CHAPTER 7: CONCLUSION AND FUTURE WORK

This chapter presents a summary of the achievements of this dissertation and integration into the state-of-the-art techniques that explore novel and bold ideas. In addition, the drawback(s) and inherent limitations of proposed techniques are discussed. Likewise, recommendations to improve design performance in terms of energy-efficiency and resilience of a few attacks are elaborated here. In the following sections, the technical summary of the elastic intermittent computation for energy-harvesting-powered devices is presented and the possible future work is also discussed.

Technical Summary

Similar to their ASIC counterparts, reconfigurable computing devices strive to surmount the growing technical challenges to improve their logic density, throughput performance, and power profiles. Thus with the geometrical and equivalent scaling trends guided by decades of ITRS projections nearing their end, new pathways towards these goals have been defined in ITRS 2.0 along with the IEEE International Roadmap for Devices and Systems (IRDS) initiative. Two such technical thrusts identified for 2020 onward are leveraging beyond-CMOS devices (ITRS 2.0 theme 5) and utilizing heterogeneous components (ITRS 2.0 theme 4) to realize fundamentally new ways to compute. The perspective taken herein is that a reconfigurable computing paradigm can significantly advance both of these declared ITRS 2.0 themes. Within the post-Moore era, there are several motivations for pursuing novel reconfigurable fabrics of heterogeneous device technologies. Foremost, their one-time design and fabrication model minimizes the recurring engineering effort for post-CMOS devices, while amortizing development costs across multiple applications. Thus, reconfigurable fabrics may offer a more cost-effective approach to utilizing emerging devices. Additionally, post-CMOS ingrained field-programmable fabrics expand the accessibility of emerging

devices to vast populations of circuit designers, including the majority of those who lack foundry access. Such a pre-fabrication approach with later field-programmability minimizes the need for extensive post-CMOS circuit design, verification, and validation expertise. Instead, heterogeneous fabrics support rapid and direct realizations in hardware. As a fundamentally different way to compute, the mapping of operations to device technologies remains fluid. Flexible mappings become possible not only during circuit synthesis, but also during execution-time. Thus when execution demands change, the architecture can adapt by utilizing a preferred device technology within its datapaths via reconfiguration of hardware components. This leverages the complementary characteristics of CMOS and emerging devices by increasing the flexibility in its binding of logic and memory roles to distinct device technologies. This is introduced herein as a post-CMOS era approach referred to as ”technology co-design.“ Overall, the hypothesis is as follows: reconfigurable fabrics of heterogeneous CMOS and spin-based devices offer an orthogonal dimension of technology adaptation to balance throughput, energy consumption, and resilience beyond static emerging device architectures, fixed hybrid emerging/CMOS architectures, and CMOS-only reconfigurable platforms.

Among promising spintronic devices, the ITRS Magnetism Roadmap identifies capable post-CMOS candidates of which STT-MTJ/SHE-MTJ, and NanoMagnetic Logic (NML) are considered feasibly-implemented. In the case of STT-MTJs, they are currently commercially available. Attributes complementary to CMOS are evident for spintronic devices, such as preferable static energy consumption, but larger write energy than CMOS. Spintronic density is higher due to 3D vertical integration capability, although its switching speed is slower. Foremost, fabric flexibility allows a direct hardware realization which encapsulates device physics and expertise needed to design circuits using the targeted nanomagnetic devices. Application-specific hardware, including energy-aware designs, are able to leverage non-volatile SHE elements at medium and fine granularities via reconfiguration. Fabrics also allow in-situ localization of data stores and datapath

re-construction at runtime based on changing execution demands and tradeoffs.

In the first step, a SPICE-compatible model for both STT-MTJ and SHE-MTJ is developed. In addition to Verilog-A and Matlab utilization, a number of realistic material parameters and physical models have been integrated into the models to achieve good agreement with experimental measurements. Two sub-models including MTJ resistive behavior and STT switching model are merged to implement STT/SHE switching approaches for both IMTJ and PMTJ -based designs. To validate the developed models, several spin-based LUTs were introduced and their functionalities are verified.

Moreover, the unifying computational mechanism underlying all of these TMR-based devices is the accumulation-mode operation that enables the realization of majority logic functions as basic computational building blocks. Therefore, we developed an evolutionary approach, SORT, to optimize the implementation of spin-based NoC circuits. The 3-input and 5-input MGs are introduced as functional building blocks and their characteristics are applied to the proposed optimization tool. First, GAs are utilized in our methodology to perform a technology-dependent optimization to generate an optimized implementation based on the obtained characteristics of spin-based building blocks. Then, complementary performance and area optimization are introduced to improve the implementation based on the requirements of the NoC system. As a proof of concept, we have developed and examined 3-input and 5-input MGs using SHE-MTJs and leveraged their characteristics to implement a functionally-complete set of Boolean logic gates. Simulation results, as well as power, delay, and area analyses verified the functionality of our proposed optimization tool for NoC circuits.

Moreover, normally-off computing using non-volatile datapaths can impart several favorable characteristics, such as anytime power-gating and high density. The overhead in comparison with the CMOS-based architectures can be justified in intermittent computing applications. Toward this

end, we proposed a systematic methodology to design NV architectures with the minimum overhead in terms of area, power, and delay. The design methodology consists of two key parts: the LE-FF, which functions as a storage and functional element and the NV-Clustering scheme, in which an optimization process has been performed. The optimized LE-FF was implemented by leveraging our SORT procedure. As a proof of concept, we have developed and examined 3-input and 5-input LE-FFs using SHE-MTJs and leveraged their characteristics to implement Boolean logic gates. We integrated and utilized two steps to explore the superiority of our methodology for a wide range of benchmarks, including ISCAS-89, ITC-99, and MCNC and compared our optimized LE-FF based designs to NV-FF implementations at the 45-nm technology node. Our proposed methodology shows an average of 15, 10, and 5 percent area reduction over NV-FF in the largescale benchmarks, ISCAS-89, ITC-99, and MCNS, respectively. Moreover, it shows a trend of better power delay product compared with NV-FF-based designs.

Finally, the non-volatility of SHE-MTJ provides a new approach against power outages during charging attacks. SIRC leverages the atomicity of the MTJ's magnetic state to realize majority logic gates, which are immune to power outage corruption down to the fine-granularity level of each logic gate. Meanwhile, data attacks are also thwarted by the same mechanism. These are combined with MG-based power masking countermeasures for possible power analysis attacks which have several advantages such as more flexibility and low area overhead in comparison to previous powermaskable units. The resulting SIRC strategy realizes intermittent-robust operability, along with energy-conserving and area-sparing features suitable for future IoT applications. Additionally, we added a new procedure to the developed NV-clustering design methodology called logic encryption step. In this step, the inserted PGs can be used for logic encryption due to their reconfigurability characteristic. Therefore, this step is defined, according to which a logic key will be generated based on Hamming distance calculations as a security metric. We applied the proposed algorithm to various benchmark circuits to evaluate the performance of our methodology in

comparison with NV-FF based implementations.

Future Work

The possible future work that can be investigated based on the work presented in this dissertation are highlighted below:

Fabrication of some selected prototypes would constitute worthwhile next steps as future work to assess the measured impact of NV-Clustering. These should target modules having characteristics which are similar to those exhibiting the most significant benefits based on the simulation of related benchmark circuits herein.

Developing more advanced genetic transformations to improve the proposed SORT framework's capability of handling larger scale optimization and synthesis.

While SHE-MTJ devices are utilized herein, any other emerging resistive devices could be leveraged without loss of generality, which can also result in further energy consumption improvements.

APPENDIX A: COPYRIGHT PERMISSIONS

Title: A Tunable Majority Gate-Based Full Adder Using Current-Induced Domain Wall Nanomagnets
Author: Arman Roohi
Publication: Magnetics, IEEE Transactions on
Publisher: IEEE
Date: Aug. 2016

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

Title: Energy-Efficient Nonvolatile Reconfigurable Logic Using Spin Hall Effect-Based Lookup Tables
Author: Ramtin Zand
Publication: Nanotechnology, IEEE Transactions on
Publisher: IEEE
Date: Jan. 2017

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Title: Voltage-Based Concatenatable Full Adder Using Spin Hall Effect Switching

Author: Arman Roohi

Publication: Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on

Publisher: IEEE

Date: Dec. 2017

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Title: Synthesis of normally-off boolean circuits: An evolutionary optimization approach utilizing spintronic devices

Conference Proceedings: 2018 19th International Symposium on Quality Electronic Design (ISQED)

Author: Arman Roohi

Publisher: IEEE

Date: March 2018

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

Title: Secure intermittent-robust computation for energy harvesting device security and outage resilience

Conference Proceedings: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM /UIC/ATC/CBDCom/IOP/SCI)

Author: Arman Roohi

Publisher: IEEE

Date: Aug. 2017

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Title: NV-Clustering: Normally-Off Computing Using Non-Volatile Datapaths
Author: Arman Roohi
Publication: Computers, IEEE Transactions on
Publisher: IEEE
Date: 1 July 2018

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Title:	Heterogeneous Technology Configurable Fabrics for Field-Programmable Co-Design of CMOS and Spin-Based Devices
Conference Proceedings:	2017 IEEE International Conference on Rebooting Computing (ICRC)
Author:	Ronald F. DeMara
Publisher:	IEEE
Date:	Nov. 2017

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

LIST OF REFERENCES

[1] L. Liu, C.-F. Pai, Y. Li, H. Tseng, D. Ralph, and R. Buhrman, "Spin-torque switching with the giant spin hall effect of tantalum," *Science*, vol. 336, no. 6081, pp. 555–558, 2012.

[2] A. Imre, G. Csaba, L. Ji, A. Orlov, G. Bernstein, and W. Porod, "Majority logic gate for magnetic quantum-dot cellular automata," *Science*, vol. 311, no. 5758, pp. 205–208, 2006.

[3] D. A. Allwood, G. Xiong, C. Faulkner, D. Atkinson, D. Petit, and R. Cowburn, "Magnetic domain-wall logic," *science*, vol. 309, no. 5741, pp. 1688–1692, 2005.

[4] B. Behin-Aein, D. Datta, S. Salahuddin, and S. Datta, "Proposal for an all-spin logic device with built-in memory," *Nature nanotechnology*, vol. 5, no. 4, p. 266, 2010.

[5] H. Meng, J. Wang, and J.-P. Wang, "A spintronics full adder for magnetic cpu," *IEEE electron device letters*, vol. 26, no. 6, pp. 360–362, 2005.

[6] J. Sun, R. W. Dave, J. A. Janesky, and J. M. Slaughter, "Magnetic tunnel junction structure and method," Aug. 11 2009, uS Patent 7,572,645.

[7] R. R. Schaller, "Moore's law: past, present and future," *IEEE spectrum*, vol. 34, no. 6, pp. 52–59, 1997.

[8] "The international technology roadmap for semiconductors," *Available at: (http://www.itrs.net)*, 2015.

[9] S. Angizi, S. Sayedsalehi, A. Roohi, N. Bagherzadeh, and K. Navi, "Design and verification of new n-bit quantum-dot synchronous counters using majority function-based jk flip-flops," *Journal of Circuits, Systems and Computers*, vol. 24, no. 10, p. 1550153, 2015.

[10] A. Roohi, S. Sayedsalehi, H. Khademolhosseini, and K. Navi, "Design and evaluation of a reconfigurable fault tolerant quantum-dot cellular automata gate," *Journal of Computational and Theoretical Nanoscience*, vol. 10, no. 2, pp. 380–388, 2013.

[11] D. E. Nikonov and I. A. Young, "Overview of beyond-cmos devices and a uniform methodology for their benchmarking," *Proceedings of the IEEE*, vol. 101, no. 12, pp. 2498–2533, 2013.

[12] X. Fong, Y. Kim, K. Yogendra, D. Fan, A. Sengupta, A. Raghunathan, and K. Roy, "Spin-transfer torque devices for logic and memory: Prospects and perspectives," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 1, pp. 1–22, 2016.

[13] J. C. Slonczewski, "Current-driven excitation of magnetic multilayers," *Journal of Magnetism and Magnetic Materials*, vol. 159, no. 1-2, pp. L1–L7, 1996.

[14] S. Wolf, D. Awschalom, R. Buhrman, J. Daughton, S. Von Molnar, M. Roukes, A. Y. Chtchelkanova, and D. Treger, "Spintronics: a spin-based electronics vision for the future," *science*, vol. 294, no. 5546, pp. 1488–1495, 2001.

[15] I. Prejbeanu, M. Kerekes, R. C. Sousa, H. Sibuet, O. Redon, B. Dieny, and J. Nozières, "Thermally assisted mram," *Journal of Physics: Condensed Matter*, vol. 19, no. 16, p. 165218, 2007.

[16] T. Devolder, C. Chappert, J. Katine, M. Carey, and K. Ito, "Distribution of the magnetization reversal duration in subnanosecond spin-transfer switching," *Physical Review B*, vol. 75, no. 6, p. 064402, 2007.

[17] H. Zhao, A. Lyle, Y. Zhang, P. Amiri, G. Rowlands, Z. Zeng, J. Katine, H. Jiang, K. Galatsis, K. Wang *et al.*, "Low writing energy and sub nanosecond spin torque transfer switching of

in-plane magnetic tunnel junction for spin torque transfer random access memory," *Journal of Applied Physics*, vol. 109, no. 7, p. 07C720, 2011.

[18] W. Kang, Z. Wang, Y. Zhang, J.-O. Klein, W. Lv, and W. Zhao, "Spintronic logic design methodology based on spin hall effect–driven magnetic tunnel junctions," *Journal of Physics D: Applied Physics*, vol. 49, no. 6, p. 065008, 2016.

[19] S. Manipatruni, D. E. Nikonov, and I. A. Young, "Energy-delay performance of giant spin hall effect switching for dense magnetic memory," *Applied Physics Express*, vol. 7, no. 10, p. 103001, 2014.

[20] D. Fan, S. Maji, K. Yogendra, M. Sharad, and K. Roy, "Injection-locked spin hall-induced coupled-oscillators for energy efficient associative computing," *IEEE Transactions on Nanotechnology*, vol. 14, no. 6, pp. 1083–1093, 2015.

[21] S. Bandyopadhyay and A. P. Chandrakasan, "Platform architecture for solar, thermal, and vibration energy combining with mppt and single inductor," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 9, pp. 2199–2215, 2012.

[22] G. Chen, M. Fojtik, D. Kim, D. Fick, J. Park, M. Seok, M.-T. Chen, Z. Foo, D. Sylvester, and D. Blaauw, "Millimeter-scale nearly perpetual sensor system with stacked battery and solar cells," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2010 IEEE International*. IEEE, 2010, pp. 288–289.

[23] H. Lhermet, C. Condemine, M. Plissonnier, R. Salot, P. Audebert, and M. Rosset, "Efficient power management circuit: From thermal energy harvesting to above-ic microbattery energy storage," *IEEE Journal of solid-state circuits*, vol. 43, no. 1, pp. 246–255, 2008.

[24] Y. K. Ramadass and A. P. Chandrakasan, "An efficient piezoelectric energy harvesting interface circuit using a bias-flip rectifier and shared inductor," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 189–204, 2010.

[25] U. Olgun, C.-C. Chen, and J. L. Volakis, "Design of an efficient ambient wifi energy harvesting system," *IET Microwaves, Antennas & Propagation*, vol. 6, no. 11, pp. 1200–1206, 2012.

[26] M. Philipose, J. R. Smith, B. Jiang, A. Mamishev, S. Roy, and K. Sundara-Rajan, "Battery-free wireless identification and sensing," *IEEE Pervasive computing*, vol. 4, no. 1, pp. 37–45, 2005.

[27] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for internet of things & sensing based applications," in *Sensing Technology (ICST), 2012 Sixth International Conference on*. IEEE, 2012, pp. 374–380.

[28] M. Imran, "Energy harvesting mechanism for medical devices," May 5 2015, uS Patent 9,026,212.

[29] S. P. Beeby, M. J. Tudor, and N. White, "Energy harvesting vibration sources for microsystems applications," *Measurement science and technology*, vol. 17, no. 12, p. R175, 2006.

[30] M. Gorlatova, J. Sarik, G. Grebla, M. Cong, I. Kymissis, and G. Zussman, "Movers and shakers: Kinetic energy harvesting for the internet of things," in *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 1. ACM, 2014, pp. 407–419.

[31] A. Poor, "Reaping the energy harvest [resources]," *IEEE Spectrum*, vol. 52, no. 4, pp. 23–24, 2015.

[32] K. Ma, Y. Zheng, S. Li, K. Swaminathan, X. Li, Y. Liu, J. Sampson, Y. Xie, and V. Narayanan, "Architecture exploration for ambient energy harvesting nonvolatile proces-

sors," in *High Performance Computer Architecture (HPCA), 2015 IEEE 21st International Symposium on*. IEEE, 2015, pp. 526–537.

[33] T. Sharma, K. Aroom, S. Naik, B. Gill, and J. X. Zhang, "Flexible thin-film pvdf-trfe based pressure sensor for smart catheter applications," *Annals of biomedical engineering*, vol. 41, no. 4, pp. 744–751, 2013.

[34] C. Chappert, A. Fert, and F. N. Van Dau, "The emergence of spin electronics in data storage," in *Nanoscience And Technology: A Collection of Reviews from Nature Journals*. World Scientific, 2010, pp. 147–157.

[35] M. N. Baibich, J. M. Broto, A. Fert, F. N. Van Dau, F. Petroff, P. Etienne, G. Creuzet, A. Friederich, and J. Chazelas, "Giant magnetoresistance of (001) fe/(001) cr magnetic superlattices," *Physical review letters*, vol. 61, no. 21, p. 2472, 1988.

[36] G. Binasch, P. Grünberg, F. Saurenbach, and W. Zinn, "Enhanced magnetoresistance in layered magnetic structures with antiferromagnetic interlayer exchange," *Physical review B*, vol. 39, no. 7, p. 4828, 1989.

[37] J. Rowell, M. Gurvitch, and J. Geerk, "Modification of tunneling barriers on nb by a few monolayers of al," *Physical Review B*, vol. 24, no. 4, p. 2278, 1981.

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

[39] D. Wang, C. Nordman, J. M. Daughton, Z. Qian, and J. Fink, "70% tmr at room temperature for sdt sandwich junctions with cofeb as free and reference layers," *IEEE Transactions on Magnetics*, vol. 40, no. 4, pp. 2269–2271, 2004.

[40] S. S. Parkin, C. Kaiser, A. Panchula, P. M. Rice, B. Hughes, M. Samant, and S.-H. Yang, "Giant tunnelling magnetoresistance at room temperature with mgo (100) tunnel barriers," *Nature materials*, vol. 3, no. 12, p. 862, 2004.

[41] W. Pratt Jr, S.-F. Lee, J. Slaughter, R. Loloee, P. Schroeder, and J. Bass, "Perpendicular giant magnetoresistances of ag/co multilayers," *Physical review letters*, vol. 66, no. 23, p. 3060, 1991.

[42] M. Julliere, "Tunneling between ferromagnetic films," *Physics letters A*, vol. 54, no. 3, pp. 225–226, 1975.

[43] Q. Xu, H. Chen, J. Lu, G. NI, and Y. DU, "Giant magnetic tunneling effect in fe/al˜ 2o˜ 3/fe," *JOURNAL OF FUNCTIONAL MATERIALS*, vol. 31, no. SUPP, pp. 42–42, 2000.

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

[45] S. Yuasa, A. Fukushima, H. Kubota, Y. Suzuki, and K. Ando, "Giant tunneling magnetoresistance up to 410% at room temperature in fully epitaxial co/ mg o/ co magnetic tunnel junctions with bcc co (001) electrodes," *Applied Physics Letters*, vol. 89, no. 4, p. 042505, 2006.

[46] S. Ikeda, J. Hayakawa, Y. Ashizawa, Y. Lee, K. Miura, H. Hasegawa, M. Tsunoda, F. Matsukura, and H. Ohno, "Tunnel magnetoresistance of 604% at 300 k by suppression of ta diffusion in co fe b/ mg o/ co fe b pseudo-spin-valves annealed at high temperature," *Applied Physics Letters*, vol. 93, no. 8, p. 082508, 2008.

[47] W. Zhao, C. Chappert, V. Javerliac, and J.-P. Noziere, "High speed, high stability and low power sensing amplifier for mtj/cmos hybrid logic circuits," *IEEE Transactions on Magnetics*, vol. 45, no. 10, pp. 3784–3787, 2009.

[48] R. Zand, A. Roohi, S. Salehi, and R. F. DeMara, "Scalable adaptive spintronic reconfigurable logic using area-matched mtj design," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 7, pp. 678–682, 2016.

[49] R. Zand, A. Roohi, D. Fan, and R. F. DeMara, "Energy-efficient nonvolatile reconfigurable logic using spin hall effect-based lookup tables," *IEEE Transactions on Nanotechnology*, vol. 16, no. 1, pp. 32–43, 2017.

[50] W. J. Gallagher and S. S. Parkin, "Development of the magnetic tunnel junction mram at ibm: From first junctions to a 16-mb mram demonstrator chip," *IBM Journal of Research and Development*, vol. 50, no. 1, p. 5, 2006.

[51] I. Prejbeanu, W. Kula, K. Ounadjela, R. Sousa, O. Redon, B. Dieny, and J.-P. Nozieres, "Thermally assisted switching in exchange-biased storage layer magnetic tunnel junctions," *IEEE Transactions on Magnetics*, vol. 40, no. 4, pp. 2625–2627, 2004.

[52] J. Hirsch, "Spin hall effect," *Physical Review Letters*, vol. 83, no. 9, p. 1834, 1999.

[53] T. Gilbert, "A lagrangian formulation of the gyromagnetic equation of the magnetization field," *Phys. Rev.*, vol. 100, p. 1243, 1955.

[54] D. C. Ralph and M. D. Stiles, "Spin transfer torques," *Journal of Magnetism and Magnetic Materials*, vol. 320, no. 7, pp. 1190–1216, 2008.

[55] A. Brataas, A. D. Kent, and H. Ohno, "Current-induced torques in magnetic materials," *Nature materials*, vol. 11, no. 5, p. 372, 2012.

[56] J. Grollier, V. Cros, A. Hamzic, J.-M. George, H. Jaffrès, A. Fert, G. Faini, J. Ben Youssef, and H. Legall, "Spin-polarized current induced switching in co/cu/co pillars," *Applied Physics Letters*, vol. 78, no. 23, pp. 3663–3665, 2001.

[57] Y. Huai, F. Albert, P. Nguyen, M. Pakala, and T. Valet, "Observation of spin-transfer switching in deep submicron-sized and low-resistance magnetic tunnel junctions," *Applied Physics Letters*, vol. 84, no. 16, pp. 3118–3120, 2004.

[58] J. Hayakawa, S. Ikeda, Y. M. Lee, R. Sasaki, T. Meguro, F. Matsukura, H. Takahashi, and H. Ohno, "Current-induced magnetization switching in mgo barrier based magnetic tunnel junctions with cofeb/ru/cofeb synthetic ferrimagnetic free layer," *Japanese journal of applied physics*, vol. 45, no. 10L, p. L1057, 2006.

[59] H. Zhao, B. Glass, P. K. Amiri, A. Lyle, Y. Zhang, Y.-J. Chen, G. Rowlands, P. Upadhyaya, Z. Zeng, J. Katine *et al.*, "Sub-200 ps spin transfer torque switching in in-plane magnetic tunnel junctions with interface perpendicular anisotropy," *Journal of Physics D: Applied Physics*, vol. 45, no. 2, p. 025001, 2011.

[60] Z. Wang, W. Zhao, E. Deng, J.-O. Klein, and C. Chappert, "Perpendicular-anisotropy magnetic tunnel junction switched by spin-hall-assisted spin-transfer torque," *Journal of Physics D: Applied Physics*, vol. 48, no. 6, p. 065001, 2015.

[61] L. Liu, C.-F. Pai, D. Ralph, and R. Buhrman, "Magnetic oscillations driven by the spin hall effect in 3-terminal magnetic tunnel junction devices," *Physical review letters*, vol. 109, no. 18, p. 186602, 2012.

[62] C.-F. Pai, L. Liu, Y. Li, H. Tseng, D. Ralph, and R. Buhrman, "Spin transfer torque devices utilizing the giant spin hall effect of tungsten," *Applied Physics Letters*, vol. 101, no. 12, p. 122404, 2012.

[63] L. Liu, T. Moriyama, D. Ralph, and R. Buhrman, "Spin-torque ferromagnetic resonance induced by the spin hall effect," *Physical review letters*, vol. 106, no. 3, p. 036601, 2011.

[64] G. H. Bernstein, A. Imre, V. Metlushko, A. Orlov, L. Zhou, L. Ji, G. Csaba, and W. Porod, "Magnetic qca systems," *Microelectronics Journal*, vol. 36, no. 7, pp. 619–624, 2005.

[65] A. Roohi, R. Zand, S. Angizi, and R. F. DeMara, "A parity-preserving reversible qca gate with self-checking cascadable resiliency," *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 4, pp. 450–459, Oct 2018.

[66] A. Roohi, H. Thapliyal, and R. DeMara, "Wire crossing constrained qca circuit design using bilayer logic decomposition," *Electronics Letters*, vol. 51, no. 21, pp. 1677–1679, 2015.

[67] W. Zhao, D. Ravelosona, J.-O. Klein, and C. Chappert, "Domain wall shift register-based reconfigurable logic," *IEEE Transactions on Magnetics*, vol. 47, no. 10, pp. 2966–2969, 2011.

[68] A. A. Khajetoorians, J. Wiebe, B. Chilian, and R. Wiesendanger, "Realizing all-spin–based logic operations atom by atom," *Science*, vol. 332, no. 6033, pp. 1062–1064, 2011.

[69] A. Lyle, S. Patil, J. Harms, B. Glass, X. Yao, D. Lilja, and J.-P. Wang, "Magnetic tunnel junction logic architecture for realization of simultaneous computation and communication," *IEEE Transactions on Magnetics*, vol. 47, no. 10, pp. 2970–2973, 2011.

[70] X. Yao, J. Harms, A. Lyle, F. Ebrahimi, Y. Zhang, and J.-P. Wang, "Magnetic tunnel junction-based spintronic logic units operated by spin transfer torque," *IEEE Transactions on Nanotechnology*, vol. 11, no. 1, pp. 120–126, 2012.

[71] B. Ransford, J. Sorber, and K. Fu, "Mementos: System support for long-running computation on rfid-scale devices," in *ACM SIGARCH Computer Architecture News*, vol. 39, no. 1. ACM, 2011, pp. 159–170.

[72] H. Jayakumar, A. Raha, and V. Raghunathan, "Quickrecall: A low overhead hw/sw approach for enabling computations across power cycles in transiently powered computers," in *VLSI Design and 2014 13th International Conference on Embedded Systems, 2014 27th International Conference on*. IEEE, 2014, pp. 330–335.

[73] B. Ransford and B. Lucia, "Nonvolatile memory is a broken time machine," in *Proceedings of the workshop on Memory Systems Performance and Correctness*. ACM, 2014, p. 5.

[74] B. Lucia and B. Ransford, "A simpler, safer programming and execution model for intermittent systems," *ACM SIGPLAN Notices*, vol. 50, no. 6, pp. 575–585, 2015.

[75] D. Balsamo, A. S. Weddell, G. V. Merrett, B. M. Al-Hashimi, D. Brunelli, and L. Benini, "Hibernus: Sustaining computation during intermittent supply for energy-harvesting systems," *IEEE Embedded Systems Letters*, vol. 7, no. 1, pp. 15–18, 2015.

[76] M. Buettner, B. Greenstein, and D. Wetherall, "Dewdrop: an energy-aware runtime for computational rfid," in *Proc. USENIX NSDI*, 2011, pp. 197–210.

[77] A. Colin and B. Lucia, "Chain: tasks and channels for reliable intermittent programs," *ACM SIGPLAN Notices*, vol. 51, no. 10, pp. 514–530, 2016.

[78] W. Brinkman, R. Dynes, and J. Rowell, "Tunneling conductance of asymmetrical barriers," *Journal of applied physics*, vol. 41, no. 5, pp. 1915–1921, 1970.

[79] W. Zhao, J. Duval, J.-O. Klein, and C. Chappert, "A compact model for magnetic tunnel junction (mtj) switched by thermally assisted spin transfer torque (tas+ stt)," *Nanoscale research letters*, vol. 6, no. 1, p. 368, 2011.

[80] N. Nishimura, T. Hirai, A. Koganei, T. Ikeda, K. Okano, Y. Sekiguchi, and Y. Osada, "Magnetic tunnel junction device with perpendicular magnetization films for high-density mag-

netic random access memory," *Journal of applied physics*, vol. 91, no. 8, pp. 5246–5249, 2002.

[81] W. Zhao, E. Belhaire, Q. Mistral, C. Chappert, V. Javerliac, B. Dieny, and E. Nicolle, "Macro-model of spin-transfer torque based magnetic tunnel junction device for hybrid magnetic-cmos design," in *Behavioral Modeling and Simulation Workshop, Proceedings of the 2006 IEEE International*. IEEE, 2006, pp. 40–43.

[82] L. Liu, T. Moriyama, D. Ralph, and R. Buhrman, "Reduction of the spin-torque critical current by partially canceling the free layer demagnetization field," *Applied Physics Letters*, vol. 94, no. 12, p. 122508, 2009.

[83] S. Ikeda, K. Miura, H. Yamamoto, K. Mizunuma, H. Gan, M. Endo, S. Kanai, J. Hayakawa, F. Matsukura, and H. Ohno, "A perpendicular-anisotropy cofeb–mgo magnetic tunnel junction," *Nature materials*, vol. 9, no. 9, p. 721, 2010.

[84] W. Kang, C. Zheng, Y. Zhang, D. Ravelosona, W. Lv, and W. Zhao, "Complementary spintronic logic with spin hall effect-driven magnetic tunnel junction," *IEEE Transactions on Magnetics*, vol. 51, no. 11, pp. 1–4, 2015.

[85] R. Koch, J. Katine, and J. Sun, "Time-resolved reversal of spin-transfer switching in a nanomagnet," *Physical review letters*, vol. 92, no. 8, p. 088302, 2004.

[86] W. F. Brown Jr, "Thermal fluctuations of a single-domain particle," *Physical Review*, vol. 130, no. 5, p. 1677, 1963.

[87] W. Zhao, E. Belhaire, C. Chappert, and P. Mazoyer, "Spin transfer torque (stt)-mram–based runtime reconfiguration fpga circuit," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 9, no. 2, p. 14, 2009.

[88] M. Krishna Gopi Krishna, A. Roohi, R. Zand, and R. F. DeMara, "Heterogeneous energy-sparing reconfigurable logic: spin-based storage and cnfet-based multiplexing," *IET Circuits, Devices Systems*, vol. 11, no. 3, pp. 274–279, 2017.

[89] Y. Zhou, S. Thekkel, and S. Bhunia, "Low power fpga design using hybrid cmos-nems approach," in *Low Power Electronics and Design (ISLPED), 2007 ACM/IEEE International Symposium on*. IEEE, 2007, pp. 14–19.

[90] W. Zhao, E. Belhaire, C. Chappert, F. Jacquet, and P. Mazoyer, "New non-volatile logic based on spin-mtj," *physica status solidi (a)*, vol. 205, no. 6, pp. 1373–1377, 2008.

[91] D. Suzuki, M. Natsui, and T. Hanyu, "Area-efficient lut circuit design based on asymmetry of mtj's current switching for a nonvolatile fpga," in *Circuits and Systems (MWSCAS), 2012 IEEE 55th International Midwest Symposium on*. IEEE, 2012, pp. 334–337.

[92] A. Alzahrani and R. F. DeMara, "Process variation immunity of alternative 16nm hk/mg-based fpga logic blocks," in *Circuits and Systems (MWSCAS), 2015 IEEE 58th International Midwest Symposium on*. IEEE, 2015, pp. 1–4.

[93] D. E. Nikonov, G. I. Bourianoff, and T. Ghani, "Proposal of a spin torque majority gate logic," *IEEE Electron Device Letters*, vol. 32, no. 8, pp. 1128–1130, 2011.

[94] M. Bonyadi, S. Azghadi, N. Rad, K. Navi, and E. Afjei, "Logic optimization for majority gate-based nanoelectronic circuits based on genetic algorithm," in *Electrical Engineering, 2007. ICEE'07. International Conference on*. IEEE, 2007, pp. 1–5.

[95] O. Boulle, G. Malinowski, and M. Kläui, "Current-induced domain wall motion in nanoscale ferromagnetic elements," *Materials Science and Engineering: R: Reports*, vol. 72, no. 9, pp. 159–187, 2011.

[96] A. Roohi, R. Zand, and R. F. DeMara, "A tunable majority gate-based full adder using current-induced domain wall nanomagnets," *IEEE Transactions on Magnetics*, vol. 52, no. 8, pp. 1–7, 2016.

[97] S. S. Parkin, M. Hayashi, and L. Thomas, "Magnetic domain-wall racetrack memory," *Science*, vol. 320, no. 5873, pp. 190–194, 2008.

[98] M. Hayashi, L. Thomas, R. Moriya, C. Rettner, and S. S. Parkin, "Current-controlled magnetic domain-wall nanowire shift register," *Science*, vol. 320, no. 5873, pp. 209–211, 2008.

[99] J. Kim, A. Paul, P. A. Crowell, S. J. Koester, S. S. Sapatnekar, J.-P. Wang, and C. H. Kim, "Spin-based computing: Device concepts, current status, and a case study on a high-performance microprocessor," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 106–130, 2015.

[100] M. Sharad, R. Venkatesan, A. Raghunathan, and K. Roy, "Multi-level magnetic ram using domain wall shift for energy-efficient, high-density caches," in *Proceedings of the 2013 International Symposium on Low Power Electronics and Design*. IEEE Press, 2013, pp. 64–69.

[101] C.-J. Yen and C.-H. Cheng, "Voltage-controlled current source," Aug. 26 2008, uS Patent 7,417,415.

[102] E. Eken, Y. Zhang, W. Wen, R. Joshi, H. Li, and Y. Chen, "A novel self-reference technique for stt-ram read and write reliability enhancement," *IEEE Transactions on Magnetics*, vol. 50, no. 11, pp. 1–4, 2014.

[103] A. S. Iyengar, S. Ghosh, and K. Ramclam, "Domain wall magnets for embedded memory and hardware security," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 1, pp. 40–50, 2015.

[104] T. Min, Q. Chen, R. Beach, G. Jan, C. Horng, W. Kula, T. Torng, R. Tong, T. Zhong, D. Tang *et al.*, "A study of write margin of spin torque transfer magnetic random access memory technology," *IEEE Transactions on Magnetics*, vol. 46, no. 6, pp. 2322–2327, 2010.

[105] Y. Seo, X. Fong, and K. Roy, "Domain wall coupling-based stt-mram for on-chip cache applications," *IEEE Transactions on Electron Devices*, vol. 62, no. 2, pp. 554–560, 2015.

[106] S. Matsunaga, J. Hayakawa, S. Ikeda, K. Miura, H. Hasegawa, T. Endoh, H. Ohno, and T. Hanyu, "Fabrication of a nonvolatile full adder based on logic-in-memory architecture using magnetic tunnel junctions," *Applied Physics Express*, vol. 1, no. 9, p. 091301, 2008.

[107] A. Roohi, R. Zand, D. Fan, and R. F. DeMara, "Voltage-based concatenatable full adder using spin hall effect switching," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 12, pp. 2134–2138, 2017.

[108] Q. An, L. Su, J.-O. Klein, S. Le Beux, I. O'Connor, and W. Zhao, "Full-adder circuit design based on all-spin logic device," in *Nanoscale Architectures (NANOARCH), 2015 IEEE/ACM International Symposium on*. IEEE, 2015, pp. 163–168.

[109] S. Khanna, S. C. Bartling, M. Clinton, S. Summerfelt, J. A. Rodriguez, and H. P. McAdams, "An fram-based nonvolatile logic mcu soc exhibiting 100% digital state retention at vdd = 0 v achieving zero leakage with ¡ 400-ns wakeup time for ulp applications," *IEEE Journal of Solid-State Circuits*, vol. 49, no. 1, pp. 95–106, 2014.

[110] M. Zwerg, A. Baumann, R. Kuhn, M. Arnold, R. Nerlich, M. Herzog, R. Ledwa, C. Sichert, V. Rzehak, P. Thanigai *et al.*, "An 82 μa/mhz microcontroller with embedded feram for energy-harvesting applications," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2011 IEEE International*. IEEE, 2011, pp. 334–336.

[111] A. Baumann, M. Jung, K. Huber, M. Arnold, C. Sichert, S. Schauer, and R. Brederlow, "A mcu platform with embedded fram achieving 350na current consumption in real-time clock mode with full state retention and 6.5 μs system wakeup time," in *VLSI Circuits (VLSIC), 2013 Symposium on*. IEEE, 2013, pp. C202–C203.

[112] T.-K. Chien, L.-Y. Chiou, C.-C. Lee, Y.-C. Chuang, S.-H. Ke, S.-S. Sheu, H.-Y. Li, P.-H. Wang, T.-K. Ku, M.-J. Tsai *et al.*, "An energy-efficient nonvolatile microprocessor considering software-hardware interaction for energy harvesting applications," in *VLSI Design, Automation and Test (VLSI-DAT), 2016 International Symposium on*. IEEE, 2016, pp. 1–4.

[113] Y. Liu, Z. Li, H. Li, Y. Wang, X. Li, K. Ma, S. Li, M.-F. Chang, S. John, Y. Xie *et al.*, "Ambient energy harvesting nonvolatile processors: from circuit to system," in *Proceedings of the 52nd Annual Design Automation Conference*. ACM, 2015, p. 150.

[114] S. Senni, L. Torres, G. Sassatelli, and A. Gamatie, "Non-volatile processor based on mram for ultra-low-power iot devices," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, no. 2, p. 17, 2017.

[115] S. Senni, L. Torres, P. Benoit, A. Gamatie, and G. Sassatelli, "Normally-off computing and checkpoint/rollback for fast, low-power, and reliable devices," *IEEE Magnetics Letters*, vol. 8, pp. 1–5, 2017.

[116] G. Prenat, K. Jabeur, P. Vanhauwaert, G. Di Pendina, F. Oboril, R. Bishnoi, M. Ebrahimi, N. Lamard, O. Boulle, K. Garello *et al.*, "Ultra-fast and high-reliability sot-mram: From cache replacement to normally-off computing." *IEEE Trans. Multi-Scale Computing Systems*, vol. 2, no. 1, pp. 49–60, 2016.

[117] D. Chabi, W. Zhao, E. Deng, Y. Zhang, N. B. Romdhane, J.-O. Klein, and C. Chappert, "Ultra low power magnetic flip-flop based on checkpointing/power gating and self-enable

mechanisms," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 6, pp. 1755–1765, 2014.

[118] R. Bishnoi, F. Oboril, and M. B. Tahoori, "Non-volatile non-shadow flip-flop using spin orbit torque for efficient normally-off computing," in *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*. IEEE, 2016, pp. 769–774.

[119] N. Sakimura, Y. Tsuji, R. Nebashi, H. Honjo, A. Morioka, K. Ishihara, K. Kinoshita, S. Fukami, S. Miura, N. Kasai *et al.*, "10.5 a 90nm 20mhz fully nonvolatile microcontroller for standby-power-critical applications," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International*. IEEE, 2014, pp. 184–185.

[120] Y. Wang, Y. Liu, S. Li, D. Zhang, B. Zhao, M.-F. Chiang, Y. Yan, B. Sai, and H. Yang, "A 3us wake-up time nonvolatile processor based on ferroelectric flip-flops," in *ESSCIRC (ESSCIRC), 2012 Proceedings of the*. IEEE, 2012, pp. 149–152.

[121] K. Shi and D. Howard, "Challenges in sleep transistor design and implementation in low-power designs," in *Proceedings of the 43rd annual Design Automation Conference*. ACM, 2006, pp. 113–116.

[122] R. Bishnoi, F. Oboril, and M. B. Tahoori, "Design of defect and fault-tolerant nonvolatile spintronic flip-flops," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 4, pp. 1421–1432, 2017.

[123] A. Roohi and R. F. DeMara, "Nv-clustering: Normally-off computing using non-volatile datapaths," *IEEE Transactions on Computers*, vol. 67, no. 7, pp. 949–959, July 2018.

[124] A. Roohi, R. Zand, and R. F. DeMara, "Synthesis of normally-off boolean circuits: An evolutionary optimization approach utilizing spintronic devices," in *2018 19th International Symposium on Quality Electronic Design (ISQED)*, March 2018, pp. 49–54.

[125] S. C. Bartling, S. Khanna, M. P. Clinton, S. R. Summerfelt, J. A. Rodriguez, and H. P. McAdams, "An 8mhz 75μa/mhz zero-leakage non-volatile logic-based cortex-m0 mcu soc exhibiting 100% digital state retention at v dd= 0v with¡ 400ns wakeup and sleep transitions," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2013 IEEE International*. IEEE, 2013, pp. 432–433.

[126] K. Jabeur, G. Di Pendina, F. Bernard-Granger, and G. Prenat, "Spin orbit torque non-volatile flip-flop for high speed and low energy applications," *IEEE electron device letters*, vol. 35, no. 3, pp. 408–410, 2014.

[127] D. Roberts, T. Kgil, and T. Mudge, "Using non-volatile memory to save energy in servers," in *Proceedings of the Conference on Design, Automation and Test in Europe*. European Design and Automation Association, 2009, pp. 743–748.

[128] Y. Liu, Z. Wang, A. Lee, F. Su, C.-P. Lo, Z. Yuan, C.-C. Lin, Q. Wei, Y. Wang, Y.-C. King *et al.*, "4.7 a 65nm reram-enabled nonvolatile processor with 6$\times$ reduction in restore time and 4$\times$ higher clock frequency using adaptive data retention and self-write-termination nonvolatile logic," in *Solid-State Circuits Conference (ISSCC), 2016 IEEE International*. IEEE, 2016, pp. 84–86.

[129] N. Sakimura, T. Sugibayashi, R. Nebashi, and N. Kasai, "Nonvolatile magnetic flip-flop for standby-power-free socs," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 8, pp. 2244–2250, 2009.

[130] T. Na, K. Ryu, J. Kim, S.-O. Jung, J. P. Kim, and S. H. Kang, "High-performance low-power magnetic tunnel junction based non-volatile flip-flop," in *Circuits and Systems (ISCAS), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 1953–1956.

[131] M. Gorlatova, J. Sarik, G. Grebla, M. Cong, I. Kymissis, and G. Zussman, "Movers and shakers: Kinetic energy harvesting for the internet of things," in *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 1. ACM, 2014, pp. 407–419.

[132] M. T. Lazarescu, "Design of a wsn platform for long-term environmental monitoring for iot applications," *IEEE Journal on emerging and selected topics in circuits and systems*, vol. 3, no. 1, pp. 45–54, 2013.

[133] A. Ma and A. S. Poon, "Midfield wireless power transfer for bioelectronics," *IEEE Circuits and Systems Magazine*, vol. 15, no. 2, pp. 54–60, 2015.

[134] Q. Alasad, J. Yuan, and D. Fan, "Leveraging all-spin logic to improve hardware security," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*. ACM, 2017, pp. 491–494.

[135] R. Zand, A. Roohi, and R. F. DeMara, "Energy-efficient and process-variation-resilient write circuit schemes for spin hall effect mram device," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 9, pp. 2394–2401, 2017.

[136] W. Zhao, C. Chappert, V. Javerliac, and J.-P. Noziere, "High speed, high stability and low power sensing amplifier for mtj/cmos hybrid logic circuits," *IEEE Transactions on Magnetics*, vol. 45, no. 10, pp. 3784–3787, 2009.

[137] H. Kimura, T. Fuchikami, K. Maramoto, Y. Fujimori, S. Izumi, H. Kawaguchi, and M. Yoshimoto, "A 2.4 pj ferroelectric-based non-volatile flip-flop with 10-year data retention capability," in *Solid-State Circuits Conference (A-SSCC), 2014 IEEE Asian*. IEEE, 2014, pp. 21–24.

[138] J. Slaughter, N. Rizzo, J. Janesky, R. Whig, F. Mancoff, D. Houssameddine, J. Sun, S. Aggarwal, K. Nagel, S. Deshpande *et al.*, "High density st-mram technology," in *Electron Devices Meeting (IEDM), 2012 IEEE International*. IEEE, 2012, pp. 29–3.

[139] J. Slaughter, K. Nagel, R. Whig, S. Deshpande, S. Aggarwal, M. DeHerrera, J. Janesky, M. Lin, H.-J. Chia, M. Hossain *et al.*, "Technology for reliable spin-torque mram products," in *Electron Devices Meeting (IEDM), 2016 IEEE International*. IEEE, 2016, pp. 21–5.

[140] R. F. DeMara, A. Roohi, R. Zand, and S. D. Pyle, "Heterogeneous technology configurable fabrics for field-programmable co-design of cmos and spin-based devices," in *Rebooting Computing (ICRC), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1–4.

[141] R. Zand, A. Roohi, D. Fan, and R. F. DeMara, "Energy-efficient nonvolatile reconfigurable logic using spin hall effect-based lookup tables," *IEEE Transactions on Nanotechnology*, vol. 16, no. 1, pp. 32–43, 2017.

[142] Q. Liu, K. S. Yildirim, P. Pawełczak, and M. Warnier, "Safe and secure wireless power transfer networks: Challenges and opportunities in rf-based systems," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 74–79, 2016.

[143] J. Kang, R. Yu, S. Maharjan, Y. Zhang, X. Huang, S. Xie, H. Bogucka, and S. Gjessing, "Toward secure energy harvesting cooperative networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 114–121, 2015.

[144] L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macii, and F. Pro, "Energy-aware design techniques for differential power analysis protection," in *Design Automation Conference, 2003. Proceedings*. IEEE, 2003, pp. 36–41.

[145] A. Roohi, R. F. DeMara, L. Wang, and S. Kse, "Secure intermittent-robust computation for energy harvesting device security and outage resilience," in *2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation*, Aug 2017, pp. 1–5.

[146] A. Roohi, R. Zand, and R. F. DeMara, "Logic-encrypted synthesis for energy-harvesting-powered spintronic-embedded datapath design," in *Proceedings of the 2018 on Great Lakes Symposium on VLSI*, ser. GLSVLSI '18. ACM, 2018, pp. 9–14.

[147] A. Stoica, R. Zebulum, and D. Keymeulen, "Polymorphic electronics," in *International Conference on Evolvable Systems*. Springer, 2001, pp. 291–302.

[148] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault analysis-based logic encryption," *IEEE Transactions on computers*, vol. 64, no. 2, pp. 410–424, 2015.

[149] Q. Alasad, Y. Bi, and J.-S. Yuan, "E2lemi: Energy-efficient logic encryption using multiplexer insertion," *Electronics*, vol. 6, no. 1, p. 16, 2017.

[150] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending piracy of integrated circuits," *Computer*, vol. 43, no. 10, pp. 30–38, 2010.

[151] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 83–89.