Subthreshold circuits: Design, implementation and application

Hrishikesh Kanitkar

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.
Subthreshold circuits: Design, Implementation and Application

by

Hrishikesh Kanitkar

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

Supervised by

Dhireesha Kudithipudi, Assistant Professor,
Dept. of Computer Engineering

Department of Electrical Engineering

Kate Gleason College of Engineering
Rochester Institute of Technology
Rochester, New York

February 2009
Title: Subthreshold circuits: Design, Implementation and Application

I, Hrishikesh Kanitkar, hereby grant permission to the Wallace Memorial Library reproduce my thesis in whole or part.

Hrishikesh Kanitkar

Date
The Thesis “Subthreshold circuits: Design, Implementation and Application” by Hrishikesh Kanitkar has been examined and approved by the following Examination Committee:

Dhireesha Kudithipudi
Assistant Professor,
Dept. of Computer Engineering
Thesis Research Adviser

Eric Peskin
Assistant Professor,
Dept. of Electrical Engineering

Marcin Lukowiak
Assistant Professor,
Dept. of Computer Engineering

Dorin Patru
Assistant Professor,
Dept. of Electrical Engineering

Vincent Amuso
Head of Department,
Dept. of Electrical Engineering
Abstract

Subthreshold circuits: Design, Implementation and Application

Hrishikesh Kanitkar

Supervising Professor: Dhireesha Kudithipudi

Digital circuits operating in the subthreshold region of the transistor are being used as an ideal option for ultra low power complementary metal-oxide-semiconductor (CMOS) design. The use of subthreshold circuit design in cryptographic systems is gaining importance as a counter measure to power analysis attacks. A power analysis attack is a non-invasive side channel attack in which the power consumption of the cryptographic system can be analyzed to retrieve the encrypted data. A number of techniques to increase the resistance to power attacks have been proposed at algorithmic and hardware levels, but these techniques suffer from large area and power overheads.

The main aim of this research is to understand the viability of implementing subthreshold systems for cryptographic applications. Standard cell libraries in subthreshold are designed and a methodology to identify the minimum energy point, aspect ratio, frequency range and operating voltage for CMOS standard cells is defined. As scalar multiplication is the fundamental operation in elliptic curve cryptographic systems, a digit-level gaussian normal basis (GNB) multiplier is implemented using the aforementioned standard cells. A similar standard-cell library is designed for the multiplier to operate in the superthreshold regime. The subthreshold and superthreshold multipliers are then subjected to a differential power analysis attack. Power performance and signal-to-noise ratio (SNR) of both these systems are compared to evaluate the usefulness of the subthreshold design. The power consumption of the subthreshold multiplier is 4.554 µW, the speed of the multiplier is 65.1 KHz and the SNR is 40 dB. The superthreshold multiplier has a power consumption of 4.005 mW, the speed of the multiplier is 330 MHz and the SNR is 200 dB. Reduced power consumption, hence reduced SNR, increases the resistance of the subthreshold multiplier against power analysis attacks.
# Contents

Abstract  ................................................................. iv

1 Thesis Overview ......................................................... 1
   1.1 Thesis Objectives ............................................... 1
   1.2 Related Work ................................................... 1
   1.3 Thesis Description .............................................. 4

2 Subthreshold Circuits .................................................. 5
   2.1 Introduction ..................................................... 5
   2.2 Modeling Transistor Current .................................. 6
   2.3 Power, Energy and Frequency .................................. 7
   2.4 Energy Point Minimization .................................... 9
   2.5 Design of a Standard Cell Library ............................ 10

3 Cryptography ............................................................. 22
   3.1 Introduction ..................................................... 22
      3.1.1 Private Key Cryptography .............................. 23
      3.1.2 Public Key Cryptography .............................. 23
      3.1.3 Elliptic Curve Cryptography ........................... 24
      3.1.4 Side Channel Attacks .................................. 24
      3.1.5 Countermeasures against side channel attacks ....... 25
   3.2 Gaussian Normal Basis Multiplier ............................ 27
      3.2.1 Mathematical Background .............................. 27
      3.2.2 Overview of the multiplier ............................ 30

4 Results and Analysis .................................................... 33
   4.1 Standard Cell Libraries ....................................... 33
      4.1.1 INVERTER ............................................... 33
      4.1.2 Universal Gates ......................................... 42
4.1.3 XOR and XNOR ................................................. 51
4.1.4 FLIP-FLOPS .................................................. 54
4.1.5 Multiple Input Gates ......................................... 58
4.1.6 AND-OR and AND-OR-INVERT Gates ...................... 75
4.1.7 OR-AND and OR-AND-INVERT Gates ....................... 94
4.1.8 NOR0211 ..................................................... 102
4.1.9 Summary of Standard Cell Library .......................... 105
4.1.10 Process variation ........................................... 108
4.2 Performance Evaluation of Multiplier .......................... 112
4.2.1 Functionality .................................................. 112
4.2.2 Effectiveness of the subthreshold operation against power analysis attacks .............................................. 114

5 Conclusions and Future Work ........................................ 120
5.1 Conclusions ..................................................... 120
5.2 Future Work .................................................... 121

Bibliography ........................................................ 122
List of Tables

2.1 Truth table for D-multiplier flip-flop. . . . . . . . . . . . . . . . . . . . . . 18
4.1 Standard cell library characteristics: combinational circuits. . . . . . . . . 106
4.2 Standard cell library characteristics: sequential circuits. . . . . . . . . . . 106
4.3 Frequency, power and delay comparison between standard cell library ele-
   ments at 300 mV. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 107
List of Figures

2.1 Transistor current characteristics. ............................................. 6
2.2 Ring oscillator power characteristics. ........................................ 8
2.3 Ring oscillator frequency characteristics. ................................. 9
2.4 INVERTER. .............................................................................. 10
2.5 Ring oscillator test circuit. ....................................................... 11
2.6 NAND. ................................................................................. 11
2.7 NOR. ....................................................................................... 11
2.8 Design methodology for subthreshold circuits. ............................ 12
2.9 Two implementations of the XOR gate (a)Tiny XOR. (b)Subthreshold XOR. 13
2.10 Tiny XOR characteristics. ....................................................... 14
2.11 XOR gate suitable for subthreshold operation. ........................... 15
2.12 Transmission gate flip-flop. .................................................... 16
2.13 Transmission gate flip-flop characteristics. ................................ 17
2.14 Modified transmission gate flip-flop. ........................................ 18
2.15 Modified transmission gate flip-flop output characteristics. ......... 19
2.16 D-multiplier flip-flop. ............................................................. 20

3.1 Abstraction levels of cryptographic systems (adapted from [23]) ........ 26
3.2 Computation of $A + B = C$. ................................................... 30
3.3 Computation of $2A = C$. ......................................................... 30
3.4 Digit-level gaussian normal basis multiplier with parallel output $DLGM_p$ (adapted from [44]). .......................................................... 31
3.5 The type 4 $DLGM_p$ over $GF(2^7)$($d = 2, r = 1$) (adapted from [44]). 32

4.1 Nominal case aspect ratio. ..................................................... 34
4.2 Worst case aspect ratio. ......................................................... 35
4.3 INVERTER energy characteristics; aspect ratio (2/1). ................. 36
4.4 INVERTER energy characteristics; aspect ratio (5/1). ................. 37
4.5 INVERTER voltage transfer characteristics. ............................ 38
4.6 Variation of minimum energy point with alpha. .......................... 39
4.7 INVERTER frequency characteristics. ........................................... 40
4.8 INVERTER power characteristics. ................................................ 41
4.9 NAND energy characteristics: aspect ratio (2/1). ......................... 43
4.10 NAND energy characteristics: aspect ratio (5/1). ....................... 44
4.11 NAND frequency comparison. .................................................... 45
4.12 NAND power comparison. ....................................................... 46
4.13 NOR energy characteristics: aspect ratio (2/1). ......................... 47
4.14 NOR energy characteristics: aspect ratio (5/1). ....................... 48
4.15 NOR frequency comparison. ..................................................... 49
4.16 NOR power comparison. .......................................................... 50
4.17 XOR gate. ............................................................................... 51
4.18 XNOR gate. .............................................................................. 51
4.19 Frequency comparison between XOR and XNOR gates. ............... 52
4.20 Power comparison between XOR and XNOR gates. .................... 53
4.21 D flip-flop frequency characteristics. .......................................... 54
4.22 D flip-flop power characteristics. ............................................... 55
4.23 D-multiplier flip-flop frequency characteristics. ......................... 56
4.24 D-multiplier flip-flop power characteristics. ............................... 57
4.25 2-input NAND gate. ................................................................. 58
4.26 3-input NAND gate. ................................................................. 58
4.27 4-input NAND gate. ................................................................. 59
4.28 Frequency comparison between 2, 3 and 4-input NAND gates. .... 60
4.29 Power comparison between 2, 3 and 4-input NAND gates. .......... 61
4.30 2-input NOR gate. ................................................................. 62
4.31 3-input NOR gate. ................................................................. 63
4.32 4-input NOR gate. ................................................................. 63
4.33 Frequency comparison between 2, 3 and 4-input NOR gates. ....... 64
4.34 Power comparison between 2, 3 and 4-input NOR gates. .......... 65
4.35 2-input AND gate. ................................................................. 66
4.36 3-input AND gate. ................................................................. 66
4.37 4-input AND gate. ................................................................. 67
4.38 Frequency comparison between 2, 3 and 4-input AND gates. ....... 68
4.39 Power comparison between 2, 3 and 4-input AND gates. .......... 69
4.40 2-input OR gate. ................................................................. 70
4.41 3-input OR gate. ................................................................. 70
4.42 4-input OR gate. .......................................................... 71
4.43 Frequency comparison between 2, 3 and 4-input OR gates. .......... 72
4.44 Power comparison between 2, 3 and 4-input OR gates. ............... 73
4.45 AOI21. ........................................................................... 75
4.46 AOI21. ........................................................................... 76
4.47 Frequency comparison between AO21 and AOI21 gates. ............ 77
4.48 Power comparison between AO21 and AOI21 gates. ................. 78
4.49 AO22. ........................................................................... 79
4.50 AOI22. ........................................................................... 80
4.51 Frequency comparison between AO22 and AOI22 gates. .......... 81
4.52 Power comparison between AO22 and AOI22 gates. ............... 82
4.53 AO32. ........................................................................... 83
4.54 AOI32. ........................................................................... 84
4.55 Frequency comparison between AO32 and AOI32 gates. .......... 85
4.56 Power comparison between AO32 and AOI32 gates. ............... 86
4.57 AO221. ......................................................................... 87
4.58 AOI221. ....................................................................... 88
4.59 Frequency comparison between AO221 and AOI221 gates. ....... 88
4.60 Power comparison between AO221 and AOI221 gates. .......... 89
4.61 AO321. ....................................................................... 90
4.62 AOI321. ....................................................................... 91
4.63 Frequency comparison between AO321 and AOI321 gates. ....... 92
4.64 Power comparison between AO321 and AOI321 gates. .......... 93
4.65 OA21. ......................................................................... 94
4.66 OAI21. ........................................................................ 95
4.67 Frequency comparison between OA21 and OAI21 gates. ......... 96
4.68 Power comparison between OA21 and OAI21 gates. ............ 97
4.69 OA32. ....................................................................... 98
4.70 OAI32. ....................................................................... 99
4.71 Frequency comparison between OA32 and OAI32 gates. ......... 100
4.72 Power comparison between OA32 and OAI32 gates. ............ 101
4.73 NOR0211. .................................................................... 102
4.74 NOR0211 frequency characteristics. . . . . . . . . . . . . . . . . . .. 103
4.75 NOR0211 power characteristics. ............................................ 104
4.76 Inverter power for positive sigma values. .............................. 108
4.77  Inverter power for negative sigma values.  . . . . . . . . . . . . . . . . . . . 109
4.78  Inverter frequency for positive sigma values.  . . . . . . . . . . . . . . . . . 110
4.79  INVERTER frequency for negative sigma values.  . . . . . . . . . . . . . . . 111
4.80  Subthreshold $DLGM_p$ output.  . . . . . . . . . . . . . . . . . . . . . . . 112
4.81  Superthreshold $DLGM_p$ output.  . . . . . . . . . . . . . . . . . . . . . . 113
4.82  Simple power analysis.  . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 115
4.83  Current traces for 1000 random input combinations at $V_{dd} = 0.3V$.  . . . 116
4.84  Current traces for 1000 random input combinations at $V_{dd} = 1.2V$.  . . . 117
4.85  Subthreshold and superthreshold multiplier power trace comparison.  . . . 118
Chapter 1

Thesis Overview

1.1 Thesis Objectives

The primary objectives of this thesis are:

- Identify the minimum energy point, aspect ratios, frequency range and operating voltage for CMOS standard cells in subthreshold and define a methodology for the design of standard cells in subthreshold.

- Design the standard cells in subthreshold.

- Use the standard cells developed to implement a digit-level GNB multiplier with parallel output.

- Perform a differential analysis attack on the subthreshold and superthreshold multipliers and compare the tradeoffs between the subthreshold and superthreshold designs with respect to area, speed, power, SNR and resistance to power analysis attacks.

1.2 Related Work

Subthreshold design for digital applications has been gaining momentum over the past decade especially in application areas where speed is not a criterion. With increasing demand for energy efficient designs, research related to subthreshold has attained considerable importance. Modeling and characterization of devices have evolved considerably with newer models being designed specifically for use in subthreshold. Substantial progress has also been made towards introducing fault tolerant and robust design techniques for subthreshold.

The concept of energy minimization and sizing of transistors for minimum energy operation for subthreshold circuits is explained in [6, 5]. These papers provide an analytical
solution for optimum supply voltage ($V_{dd}$) and threshold voltage ($V_{th}$) required to minimize energy for a given frequency of operation. To support their claim, the authors implement a FIR filter with minimum energy sized devices. The authors in [27, 26] provide a closed-form solution for sizing transistors in a stack and introduce a new logical effort [50] scheme suitable to subthreshold design. Various logic families apart from standard CMOS have also been considered for their usefulness in subthreshold design. Some of the traditional logic families like domino [48], pass transistor logic [35] and pseudo $n$-channel metal-oxide-semiconductor (nMOS) are studied for their subthreshold operation. The subdomino logic has the advantage of low power consumption and high speed as compared to its CMOS counterpart. In [35], static and dynamic subthreshold pass transistor logic XOR gates are studied, and it is concluded that dynamic-pass-transistor logic is more sensitive to process variations than normal pass transistor logic. New logic families like dual $V_T$ self-timed logic [21], variable threshold voltage subthreshold CMOS [49], subthreshold dynamic threshold voltage MOS [49] and source-coupled logic [51] are proposed for their superior tolerance to process and temperature variations. Several low power design approaches like multiple-threshold complementary metal-oxide-semiconductor (MTCMOS), partial dynamic voltage-scaling (DVS), partial DVS with MTCMOS and Insomniac and their usefulness in energy efficient design are discussed in [4]. The authors conclude that among all the low power design approaches Insomniac provides the highest energy savings.

Considerable amount of effort has been spent in finding the “perfect transistor” for operation in subthreshold. Apart from optimization of the bulk metal-oxide semiconductor field-effect transistor (MOSFET) [40, 41, 3], silicon-on-insulator (SOI) MOSFET [38, 22, 55, 54, 58], double gated MOSFET [29] and metal epitaxial semiconductor field effect transistor (MESFET) [10] have gained popularity for their usage in subthreshold design. SOI MOSFETs have the distinct advantage of steeper subthreshold slope and more resistance to short-channel effects like drain induced barrier leakage (DIBL). The authors in [29] propose that double gated MOSFET could be used in subthreshold due to its steep subthreshold slope and a small gate capacitance. As in superthreshold, process variations have a considerable effect on subthreshold designs. The analysis and impact of process variations [56, 33] and leakage energy [25, 36] have been studied and various techniques like pipelining, temperature adaptive dynamic voltage supply tuning, MTCMOS, variable threshold complementary metal-oxide semiconductor (VTCMOS), source biasing and dual $V_T$ partitioning are suggested to ameliorate these effects.

Application areas in subthreshold are not only restricted to the digital domain but have also been expanded to the analog and mixed signal domain [7]. The authors in [7] propose the use of dual-material-gate (DMG) p-MOSFET for the use in analog filter applications. Using DMG p-MOSFET, a 70% improvement in gain was observed for CMOS amplifiers.
Voltage regulators [15, 52] and low noise amplifiers (LNA) [12] have also been implemented in subthreshold. In the digital domain, subthreshold circuits are being used in static random access memory (SRAM) arrays [18, 43, 8], dynamic random access memory (DRAM) [21], fast fourier transform (FFT) processors [53], hearing aids [28], and sensor nodes [17].

The concept of power analysis attacks on cryptographic systems was proposed by Kocher [32] in the mid 1990s. A power analysis attack is a non-invasive side channel attack in which the power consumption of the cryptographic system can be analyzed to retrieve the encrypted data [32]. An attacker can mount a power attack on a system without having any knowledge of its design. Various design techniques at algorithmic and hardware levels of abstraction have been proposed as countermeasures to power analysis attacks. The typical countermeasures used in elliptic curve cryptography (ECC) at algorithmic level are the ones proposed in [31]: randomization of the private exponent, blinding the point and randomized projective co-ordinates. The authors in [24] propose the use of random elliptic curve isomorphism as an effective counter measure. [57] uses a window based approach whereas [47] exploits parallelism in the elliptic curve digital signature algorithm (ECDSA) to increase resistance against power attacks. At circuit level, hiding and masking are two popular counter measures implemented that increase the resistance against power attacks by achieving constant power consumption in every clock cycle of the system. Hiding can be implemented using dual rail logic, asynchronous logic and current mode logic, whereas masking requires dual pre-charge logic [42]. The major disadvantage of hiding and masking is that they require capacitive balancing of cells and wires at layout level in order to achieve constant power consumption. These techniques also suffer from excess area and power overheads. An ultra low voltage logic (ULV) using floating gates has been proposed in [16] due to its high speed and low-correlation between the input pattern and supply current thus making the encryption scheme more resistant to power attacks. The use of subthreshold circuits in cryptographic applications like electronic passports, where security and power consumption rather than performance are given high priority, is suggested in [16]. A subthreshold substitute bytes box (S-box) of the advanced encryption standard (AES) [9] is presented in [1]. The authors use pipelining and asynchronous subthreshold logic to implement the S-box.

The authors in [32] suggest that reducing the signal amplitude can be an effective solution in increasing resistance against power attacks. Thus, by operating a cryptographic system at subthreshold, the signal amplitude, and hence the power consumption, is reduced significantly. With this reduced signal amplitude, the variation in power consumption is difficult to measure thereby increasing the resistance against power attacks. The use of subthreshold in cryptographic systems is still nascent. With the untapped potential of
ECC systems in cryptographic applications, it is even more pertinent to study subthreshold design for ECC systems. The proposed work aims at studying the viability of using subthreshold design techniques in implementing an ECC system. As scalar multiplication is the fundamental operation in elliptic curve systems, a \textit{digit-level gaussian normal basis multiplier with parallel output} (\textit{DLGM}_p) [44] will be implemented and tested against power attacks through simulations.

### 1.3 Thesis Description

The primary focus of this research is to evaluate the usefulness of subthreshold design techniques in elliptic curve cryptography in order to increase the resistance against power attacks. As scalar multiplication is one of the basic operations in ECC, this thesis uses the \textit{DLGM}_p presented in [44].

To implement the \textit{DLGM}_p in subthreshold, first the minimum energy point, aspect ratios, frequency range and operating voltage for main components of the multiplier are identified. The basic idea is to create a standard library consisting of INVERTER, NAND, NOR, XOR gates and latches using IBM 65nm technology with $1 \times$, $2 \times$ and $3 \times$ \textit{fan-out of 4} (FO4) [20] delays. These standard cells then form the building blocks of the \textit{DLGM}_p. A similar standard cell library is also created for the multiplier to operate in the superthreshold regime. A \textit{differential power analysis} (DPA) is then performed on the subthreshold and superthreshold multipliers and their resistance to power attacks is compared. DPA can be performed on both the circuits by evaluating power traces for all the possible input combinations of the multiplier. Tradeoffs between power consumption, SNR, speed, area and resistance to power attacks of the subthreshold and superthreshold multipliers are then compared to evaluate the usefulness of the subthreshold design.
Chapter 2

Subthreshold Circuits

This chapter begins with an introduction to subthreshold circuits. It then explains the behavior of a transistor in the subthreshold region of operation. The difference between power, energy and frequency of operation in subthreshold and superthreshold circuits is explained. The penultimate section of this chapter explains the important concept of energy minimization. The chapter ends with the explanation of the design of standard cell library in subthreshold.

2.1 Introduction

With shrinking technology sizes, energy efficiency has become a critical aspect of designing digital circuits. Traditionally, voltage scaling, a mechanism in which the supply voltage is varying and the threshold voltage is constant, has been an effective solution in meeting stringent energy requirements. However, voltage scaling does come at a cost of reduction in performance. The limits of voltage scaling, and therefore energy minimization, can be explored by operating a circuit at subthreshold [19]. In subthreshold circuits, the supply voltage is reduced well below the threshold voltage of a transistor. Due to the quadratic reduction in power with respect to the supply voltage, subthreshold circuits are classified as ultra low power circuits. Specifically in application areas where performance can be sacrificed for low power, subthreshold circuits are an ideal fit. Some of the applications include devices such as hearing aids [28], wrist watches [14], radio frequency identification (RFID), sensor nodes and battery operated devices such as cellular phones. One of the major areas where subthreshold design can be exploited is cryptographic systems. Due to their extremely low power levels, subthreshold circuits provide an effective solution to power analysis attacks [32] in cryptographic systems.
2.2 Modeling Transistor Current

The region of operation of a transistor depends on the supply voltage at which it operates. As the supply voltage is reduced, the region of operation shifts from strong inversion to moderate inversion and finally to weak inversion. The strong inversion region, also known as the superthreshold regime, is characterized by large current drives and a supply voltage substantially above $V_{th}$, the threshold voltage of the transistor. The moderate inversion has lower current drives as compared to the superthreshold regime and an operating voltage near to the $V_{th}$. The weak inversion region, also known as the subthreshold regime, is characterized by small current drives and a supply voltage below $V_{th}$.

The behavior of the transistor in the subthreshold and superthreshold regions is shown in equations (2.1) and (2.2) [19]

$$I_{on-sub} = \frac{W}{L_{eff}} \mu_{eff} C_{ox} (m - 1)V_{T}^2 \exp \left( \frac{V_{gs} - V_{th}}{mV_{T}} \right) (1 - \exp \left( -\frac{V_{ds}}{V_{T}} \right))$$  \hspace{1cm} (2.1)

where $W$ is the width of the transistor, $L_{eff}$ is the effective length, $\mu_{eff}$ is the effective mobility, $C_{ox}$ is the oxide capacitance, $m$ is the subthreshold slope factor and $V_{T} = \left( \frac{KT}{q} \right)$.

$$I_{on-super} = \frac{g_{msat}}{1 + R_{s}g_{msat}} (V_{dd} - V_{th} - V_{PO})$$ \hspace{1cm} (2.2)

where $g_{msat}$ is the saturation transconductance, $R_{s}$ is the source resistance and $V_{PO}$ is the pinch off voltage.

Figure 2.1: Transistor current characteristics.

The subthreshold and superthreshold regions of operation are highlighted in Figure 2.1. In the superthreshold region, the current is fairly linear in nature. The transistor current $I_{on}$ in the subthreshold regime is exponentially dependent on $V_{th}$ and supply voltage due
to which power, delay and current matching between two transistors is also exponentially
dependent on $V_{th}$ and $V_{dd}$. This exponential dependence is a key challenge in designing
circuits in subthreshold. Some of the parameters that are affected by this challenge are
process variations, noise margins, soft errors and output voltage swings. Therefore, when
designing energy optimal subthreshold circuits, these parameters play an important role.

The current in the subthreshold region, also known as leakage current, is considered to
be undesirable when operating the transistor in the superthreshold region. However, this
current is quintessential as far as subthreshold operation is concerned. Leakage current is
utilized by subthreshold circuits as their conduction current.

### 2.3 Power, Energy and Frequency

The total power in a CMOS circuit is given by equation (2.3):

$$P_{Total} = P_{dynamic} + P_{static} = \frac{1}{2}C_LV_{dd}^2\alpha f + I_{SC}V_{dd} + I_{static}V_{dd}$$  \hspace{1cm} (2.3)

where $C_L$ is the load capacitance, $f$ is the frequency of operation, $I_{SC}$ is the short circuit
current and $\alpha$ is the activity factor. As can be seen from Equation (2.3) the total power cons-
ists of two major components: dynamic power and leakage power. Both these components
reduce in magnitude as the supply voltage reduces.

The dynamic power consumption is due to the charging and discharging of the load
capacitance and the short circuit current. A short circuit current flows when the pull up
and pull down networks in a CMOS circuit are simultaneously on and a direct path exists
between the supply line and ground. Dynamic power is directly proportional to the square
of the supply voltage. Therefore, dynamic power reduces in a quadratic manner when the
supply voltage is reduced. Leakage power is dependent on the leakage current flowing in
the CMOS circuit.

At superthreshold, the charging (or discharging) current is greater than the leakage
current. Hence, dynamic power dominates over leakage power in superthreshold. At sub-
threshold, supply voltage is lower than the threshold voltage of the transistor. Due to its
quadratic relation with supply voltage, dynamic power reduces drastically in subthreshold.
Also, leakage current is regarded as the conduction current in subthreshold. Therefore,
leakage power dominates than dynamic power in the subthreshold region of operation.

Energy is one of the important design metrics in digital circuits. The energy estimation
in these circuits is given by Equation (2.4):

$$E_{Total} = E_{dynamic} + E_{static} = \frac{1}{2}C_LV_{dd}^2\alpha + I_{static}V_{dd}t_p$$  \hspace{1cm} (2.4)

where $C_L$ is the load capacitance, $t_p$ is the circuit delay and $\alpha$ is the activity factor.
The important observation in Equation (2.4) is the dependence of leakage energy on delay \( t_p \). Since \( t_p \) is high in subthreshold, the leakage energy is greater than the dynamic energy. As the supply voltage is increased, the delay and hence the leakage energy, reduces. Therefore, at superthreshold the dynamic energy is the more dominant of the two. Short circuit energy is negligible at subthreshold and can be ignored [19].

To understand the variation in power and frequency characteristics in superthreshold and subthreshold regions, simulations of a seven-stage ring oscillator using an inverter chain were performed in IBM 65 nm technology node. The power and frequency characteristics of the ring oscillator are shown in Figure 2.2 and Figure 2.3, respectively.

![Figure 2.2: Ring oscillator power characteristics.](image)

As can be observed from the graphs, both, power and frequency increase exponentially with supply voltage. With an increase in supply voltage from 200 mV to 700 mV, a 7000x increase in power and a 700x increase in frequency are observed. Thus, the advantage of low power in the subthreshold region comes at a cost of reduced speed of operation.
Figure 2.3: Ring oscillator frequency characteristics.

2.4 Energy Point Minimization

Since energy minimization is the enabling factor for subthreshold design, identifying the operating voltage range for the optimal energy forms the design basis. Two commonly used terms in subthreshold design are $V_{min}$, the voltage at which the energy of the circuit is minimum and $V_{dd,limit}$, the lowest supply voltage at which the circuit can be operated. In most cases the $V_{min}$ is greater than $V_{dd,limit}$. $V_{min}$ denotes the ideal supply voltage at which the circuit should be operated. Stacking of transistors raises the $V_{dd,limit}$ of a circuit well above that of a simple inverter. The location of the energy minimum of any circuit is a compromise between the dynamic and leakage energies. The point of intersection of the dynamic and leakage energy curves is defined as the minimum energy point of the circuit. The activity factor, $\alpha$, $V_{th}$, $L_{eff}$, sub-$V_{th}$ slope and $I_{on}$ are interdependent and should be considered for determining the minimum energy point of any design. The main goal of
this research is to identify the minimum energy point, aspect ratios, frequency range and operating voltage for CMOS standard cells.

2.5 Design of a Standard Cell Library

This section describes the design of various digital logic cells in subthreshold. A methodology for designing a standard cell library in subthreshold is discussed. All the logic cells are verified for their performance characteristics. One of the primary reasons to form a standard cell library is to use these cells as basic building blocks for larger circuits.

The standard cell library created consists of 32 CMOS gates designed using IBM 65nm technology with 1×, 2× and 3× FO4 delays. First, the basic CMOS inverter, shown in Figure 2.4, is analyzed in detail and then, based on this analysis, the NAND and the NOR gates are designed. A seven-stage ring oscillator is used as a test circuit for the INVERTER, NAND and NOR gates. The ring oscillator test circuit is shown in Figure 2.5. The inverter is initially simulated for optimal sizing, i.e., the “ideal” aspect ratio (ratio of pMOS to nMOS width) at which the charging and discharging currents are equal and a symmetrical output is observed. The simulations are carried out for both worst case and nominal case. Nominal case process simulations imply operating the circuit at 27°C. Worst case process simulations include SS (slow nMOS, slow pMOS), SF (slow nMOS, fast pMOS), FS (fast nMOS, slow pMOS) and FF (fast nMOS, fast pMOS) corners. The optimal sizing does not necessarily mean that the circuit operates at minimum energy. Therefore, the INVERTER is re-sized and re-simulated to find the minimum energy point. The simulations are also carried out for various activity factors.
With INVERTER as the reference, the NAND and NOR gates are designed and simulated for minimum energy. The effect of increasing aspect ratio and transistor activity factor $\alpha$ on the minimum energy point are also observed. The schematic of the NAND gate and NOR gate is shown in Figure 2.6 and Figure 2.7 respectively. The methodology can be summarized by the flowchart shown in Figure 2.8.
Figure 2.8: Design methodology for subthreshold circuits.
Figure 2.9: Two implementations of the XOR gate (a)Tiny XOR. (b)Subthreshold XOR.

The design of the remaining standard cells, except the exclusive-OR (XOR) and flip-flops, is based on the results of the INVERTER, NAND and NOR gates. For designing the XOR, XNOR and the flip-flops a different approach is used. The TINY XOR (Figure 2.9(a)), commonly used in standard cell libraries, is simulated for its subthreshold operation.

The simulation of the TINY XOR gate is shown in Figure 2.10. At a voltage of 100mV or lower, the tiny XOR gate fails to operate correctly when the input bits $B$ changes from 1 to 0. For $B = 0$ and $A = 1$, the transistor $M_1$ tries to pull the output $C$ to $V_{dd}$. Transistors $M_2$, $M_3$ and $M_4$ are in parallel and try to pull the output towards ground. The combined effort of $M_2$, $M_3$ and $M_4$ overrides that of $M_1$ and hence the output rises to an intermediate value. Minimum aspect ratio of (1/1) (i.e. (W/L) for pMOS = (65 nm/65 nm) and (W/L) for nMOS = (65 nm/65 nm)) for the transmission gate and aspect ratio (2/1) (i.e. (W/L) for pMOS = (130 nm/65 nm) and (W/L) for nMOS = (65 nm/65 nm)) for the inverter is used for simulations. An increase in the aspect ratio does not change the simulation output. An XOR gate suitable for subthreshold operation is shown in Figure 2.9(b). This XOR gate uses transmission gate logic. The transmission gates are designed with an aspect ratio of (1/1). As the results in Figure 2.11 indicate, this gate is suitable for all input combinations at very low voltages. The results of the XOR gate were used to design the XNOR gate.
Figure 2.10: Tiny XOR characteristics.
Figure 2.11: XOR gate suitable for subthreshold operation.
For the design of the D flip-flop, an approach similar to the one for XOR gate is used. Initially, a transmission gate based flip-flop, shown in Figure 2.12, is simulated. The optimal aspect ratio of \((9/1)\) (\(i.e.\) \((W/L)\) for \(pMOS = (585 \text{ nm}/65 \text{ nm})\) and \((W/L)\) for \(nMOS = (65 \text{ nm}/65 \text{ nm})\)) is used for sizing the inverters and for the transmission gates a minimum sizing of \((1/1)\) is used. As can be seen from the simulations of this latch (Figure 2.13), the output of the flip-flop follows the input, but, does not rise to the required 90% noise margin.
Figure 2.13: Transmission gate flip-flop characteristics.
Figure 2.14: Modified transmission gate flip-flop.

<table>
<thead>
<tr>
<th>PREZ</th>
<th>CLRZ</th>
<th>CLK</th>
<th>D</th>
<th>Q</th>
<th>QBAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>H</td>
<td>X</td>
<td>X</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>H</td>
<td>L</td>
<td>X</td>
<td>X</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>X</td>
<td>X</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>↑</td>
<td>H</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>↑</td>
<td>L</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>L</td>
<td>X</td>
<td>(Q_0)</td>
<td>(QBAR_0)</td>
</tr>
</tbody>
</table>

In order to pull the output up to the desired value two charge keepers, one at the output node and one in the feedback loop, are needed. This modified transmission gate flip-flop is shown in Figure 2.14. Minimum sizing of 1 is used for the charge keepers. The simulations of this modified transmission gate flip-flop are shown in Figure 2.15. As can be seen from Figure 2.15, with the help of the two charge keepers, the output is pulled up to the desired 90% noise margin. For implementing the digit level gaussian normal basis multiplier the inputs need to be circularly shifted. For the multiplication process, the multiplier and the multiplicand in the input registers need to be stable for the first clock cycle. The circular shift with the above D flip-flop was implemented and it was noted that the inputs do not remain stable for the first clock cycle. Hence, a flip-flop with preset and clear pins is required. This flip-flop, the D-multiplier flip-flop, is shown in Figure 2.16 and the truth table is shown in Table 2.1.

Minimum sizing was used for the INVERTER, NAND and TRANSMISSION gates in...
Figure 2.15: Modified transmission gate flip-flop output characteristics.
Figure 2.16: D-multiplier flip-flop.
the design. For the transistor level schematics shown an inverter aspect ratio of (2/1) \(i.e.\)
\((W/L)\) for pMOS = (130 nm/65 nm) and \((W/L)\) for nMOS = (65 nm/65 nm)) was used.
Chapter 3

Cryptography

This chapter begins with an introduction to cryptography. It then explains private key, public key and elliptic curve cryptography. Side-channel attacks are then introduced with more emphasis given on power analysis attacks. The concluding section of this chapter explains the working of the gaussian normal basis multiplier. The last section also gives an overview of the mathematical background necessary for understanding the working of this multiplier.

3.1 Introduction

Cryptography is the practice and study of hiding information. The basic aim of cryptography is to ensure secure transmission of data against eavesdropping. In [46], cryptography is defined as “the discipline that studies the mathematical techniques related to information security such as providing the security services of confidentiality, data integrity, authentication and non-repudiation”. A cipher is a cryptographic algorithm that uses a key to transform the data to be transmitted, also known as the plaintext, into an unreadable form, the cipher text. Cryptography involves two processes: encryption and decryption. Encryption uses a cipher and a key to convert the plaintext data into cipher text at the transmission end. Similarly, at the receiver, decryption is performed which uses the same key to convert the cipher text data back to the original form.

Two major types of cryptographic systems are private key cryptography or symmetric cryptography and public key cryptography or asymmetric key cryptography. These systems can best be explained with the classic example of Alice, Bob and Eve. Bob would like to transfer data to Alice through an insecure channel. Eve, the eavesdropper, is trying to intercept this information. Without the means of a cryptographic algorithm, Bob’s data can be easily intercepted by Eve and Eve could then send out wrong information to Alice.
3.1.1 Private Key Cryptography

Private key cryptography uses the same key to encrypt and decrypt the message. Bob uses a key and an encryption algorithm to encipher the plaintext and transfer it to Alice. Alice uses the same key and a decryption algorithm to decipher Bob’s data. Since Eve does not have knowledge about the key, she is unable to decrypt the information. One of the most popular block cipher algorithms is the data encryption algorithm (DEA) defined in the data encryption standard (DES) [37]. The DEA uses a 56 bit secret key. An advanced version of the DEA is the Triple DEA which uses three 56 bit length keys to encrypt data. If all the keys are independent then this is called three key TDEA (3TDEA). If two keys are independent and the third key is a copy of one of the two keys it is called two key TDEA (2TDEA) [2]. In 2000, the national institute of standards and technology (NIST) [39] chose “Rijndael” as the new advanced encryption standard (AES) [9].

Private key cryptography encryption and decryption algorithms are computationally non-intensive. One of the properties of private key cryptography is that since the same key is required for encryption and decryption, a secure channel must exist between two communicating entities for the transmission of the secret key. Thus, an effective key management system is necessary. The complexity of this key management system increases with the increase in the number of entities in the network.

3.1.2 Public Key Cryptography

Public key cryptography uses two keys, mathematically related to one another, for encryption and decryption. Each entity will have its own private key and will share a public key with other entities. One of the keys is used for encryption and the other for decryption. A public key cryptographic algorithm works as follows. Bob transmits data to Alice using a public key and his private key. Alice can easily decipher Bob’s encrypted data by using her private key. Eve knows the public key but does not have any knowledge of Alice’s private key, thus she cannot decrypt Bob’s data. The security of a public key system lies in the fact that it is computationally infeasible to construct one key from the other, even though both the public and private keys are necessarily related. Also public key cryptography eliminates the need of a secure communication channel to transmit private keys. Diffie and Hellman [11] were the first to publish the concepts of public key cryptography. Public key cryptography can also be used to implement digital signatures. The current industry standard for public key cryptography is the Rivest-Shamir-Adleman (RSA) algorithm [45].
3.1.3 Elliptic Curve Cryptography

The use of elliptic curves in cryptography was proposed independently by Koblitz [30] and Miller [34]. Elliptic curve cryptography (ECC), also a public key cryptography algorithm, involves the use of points on elliptic curves over a finite field for encryption and decryption. Cryptographic algorithms using elliptic curves are more complex than the standard RSA algorithm but provide the same level of security while using a smaller key size. Thus, ECC has the advantages of requiring less storage space, small bandwidth demands and a faster key exchange. Scalar multiplication is the fundamental operation used in ECC where a point $P$ on an elliptic curve defined over a finite field is multiplied by a scalar $k$. A special case of normal basis, the $T$ type gaussian normal basis (GNB) is used for finite field multiplication. Using GNBs reduces complexity thereby providing an efficient and simple implementation of the scalar multiplication [44]. The GNBs have been included in a number of standards, such as IEEE [13] and NIST for the elliptic curve digital signature algorithm (ECDSA). The IEEE standard for implementing ECC is the elliptic curve integrated encryption scheme (ECIES).

The elliptic curve discrete logarithm problem (ECDLP) ensures the security of elliptic curve cryptographic systems. Consider an elliptic curve $E$ defined over a galois field $GF(p^m)$. Let $Q$ and $P$ be two points of this curve. Let the order of $P$ be $r$. The logarithm problem can be formulated as follows. Find a positive scalar $k \epsilon [1, r - 1]$ such that the scalar multiplication equation $Q = kP$ holds true. Solving the discrete logarithm problem over elliptic curves is said to be a very difficult mathematical exercise [46]. Scalar multiplication is used key generation, signature and verification schemes, the three fundamental ECC primitives.

3.1.4 Side Channel Attacks

A side channel attack is an attack on the physical implementation of a cryptographic system. Timing information, electromagnetic radiation and power consumption are side channels that can be exploited to gain information of the cryptographic system.

The amount of time required to complete a cryptographic operation depends on the type of operation performed. A timing attack exploits this vulnerability. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems [32]. One of the countermeasures against timing attacks would be to ensure that all operations require the same amount of time.

A power analysis attack is a non-invasive side channel attack in which the power consumption of the cryptographic system can be analyzed to retrieve the encrypted data [32]. An attacker can mount a power attack on a system without having any knowledge of its
design. The amount of power consumed in an integrated circuit is proportional to the type of operation performed and the input data pattern of the micro-processor. This is because the switching of the individual transistors of the circuit depends upon the change in the input data and the number of instructions executed depends upon the operation performed. Hence, by tracking the amount of power consumed, an attacker can easily decrypt a cryptographic system. Power analysis attacks are of two types: simple power analysis (SPA) attacks and differential power analysis (DPA) attacks [32]. In SPA attacks, the attacker observes the variation in power consumption of the micro-processor over a period of time. DPA is a more severe attack than the SPA, in which the attacker uses statistical methods and error correction techniques to determine information related to the encrypted data. DPA is much more difficult to prevent than the SPA. Other side channels attacks include those in which electro-magnetic radiation and timing information of the system are exploited by the attacker to reveal the secret key.

Reducing signal size and introducing noise can be an effective solution in increasing resistance against power attacks [32]. This is because by reducing the SNR, the attacker requires large amount of sample data, in some cases infinitely large number of samples, to implement the attack. Subthreshold power consists of 80% leakage power and 20% active power. Power corresponding to useful computation (active power) in subthreshold is insignificant as compared to super threshold where active power corresponds to 99% of the total power consumed. Inherently, the SNR of a subthreshold system is significantly lower than its superthreshold counterpart. Thus, subthreshold cryptographic systems are less prone to power analysis attacks, as the reduced supply voltage and larger leakage current guarantee power variations and SNR that are order of magnitudes less than those in the superthreshold case and hence are much more difficult to measure.

Flow of current in an electronic circuit produces magnetic field. Thus, all electronic circuits emit electromagnetic radiation. An electromagnetic analysis (EMA), similar to power analysis can be performed on the cryptographic circuit to extract information. The EMA is also of two types: simple EMA and a differential EMA. EMA attacks can extract much more information that the power analysis attacks.

3.1.5 Countermeasures against side channel attacks

Cryptographic systems can be designed at various levels of abstraction. The five primary levels of abstraction of a cryptographic embedded system are shown in Figure 3.1.

The protocol level consists of designing protocols that implement basic cryptographic functions such as data integrity, confidentiality, authentication, identification and non-repudiation. The algorithmic level consists of implementing algorithms such as block
ciphers, RSA, DES, AES, etc. At the architecture level, instruction set modeling, in programming languages such as C, C++ and JAVA, is used to design cryptographic systems. At the micro-architecture level, cryptographic systems are implemented using a higher level of hardware abstraction. Hardware description languages such as Verilog and VHDL are used to define memories, processors and co-processors. At the circuit level, transistors and gates are used to define the cryptographic system.

Countermeasures against side channel attacks are devised so as to either reduce or completely eliminate the amount of information leaked by the side channel. Various design techniques have been proposed at algorithmic and hardware levels of abstraction. Randomization of the private exponent, blinding the point and randomized projective co-ordinates are typical countermeasures used in ECC at algorithmic level [31]. The use of random elliptic curve isomorphism as an effective counter measure is proposed in [24]. [57] uses a window based approach whereas [47] exploits parallelism in the ECDSA to increase resistance against power attacks. At circuit level, hiding and masking are two popular counter measures implemented that increase the resistance against power attacks by achieving constant power consumption in every clock cycle of the system. Hiding can be implemented using dual rail logic, asynchronous logic and current mode logic, whereas masking requires dual pre-charge logic [42]. The major disadvantage of hiding and masking is that they require capacitive balancing of cells and wires at layout level in order to achieve constant power consumption. These techniques also suffer from excess area and power overheads. An ultra low voltage logic (ULV) using floating gates has been proposed in [16] due to its high speed and low-correlation between the input pattern and supply current thus making the encryption scheme more resistant to power attacks. The use of subthreshold circuits in
cryptographic applications like electronic passports, where security and power consumption rather than performance are given high priority, is suggested in [16]. A subthreshold S-box of the AES is presented in [1]. The authors use pipelining and asynchronous subthreshold logic to implement the S-box.

The authors in [32] suggest that reducing the signal amplitude can be an effective solution in increasing resistance against power attacks. Thus, by operating a cryptographic system at subthreshold, the signal amplitude, and hence the power consumption, is reduced significantly. With this reduced signal amplitude, the variation in power consumption is difficult to measure thereby increasing the resistance against power attacks.

3.2 Gaussian Normal Basis Multiplier

3.2.1 Mathematical Background

This section gives an overview of the mathematical background needed to understand the working of the gaussian normal basis multiplier.

Finite Fields

Basic definition of Rings and Fields is introduced to understand finite fields.

Rings

A set of objects that can be added and multiplied is called a ring. The objects of the ring $R$ should satisfy the following conditions:

- Under addition, the ring $R$ is an additive (Abelian) group.
- $\forall a, b, c \in R, a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.
- $\forall a, b, c \in R, a(bc) = abc$.
- $\exists$ an element $i \in R$ such that $ia = ai = a \forall \in R$.

Integers, complex numbers, real numbers and rational numbers are all rings. A number $a$ has a multiplicative inverse in $R$ and is said to be invertible if and only if there exists a unique number $x \in R$ such that $ax = xa = 1$. The unit element of the ring is 1.

Fields

A field $F$ is a ring in which the following conditions are satisfied:

- $F$ is commutative with respect to addition.
- $F$ holds all distributive laws mentioned for rings.
\( F \) is commutative with respect to multiplication.

From the definition of rings and fields, finite fields can now be defined. A finite field or Galois field is denoted by \( GF(p^m) \), where \( p \), a prime, is known as the characteristic of the field, \( m \) is a positive integer and \( p^m \) is the number of elements of the field. Ground field or subfield of the finite field consists of \( p \) number of elements of the field. This thesis focuses on \( GF(2^m) \), i.e. galois fields of order 2, also known as binary finite fields.

**Finite Field Representation**

Finite fields can be represented in a number of ways. The normal basis representation and the polynomial representation are two of the most commonly used representations.

**Polynomial Representation** An element of finite field \( GF(2^m) \) can be represented by the polynomial equation (3.1).

\[
b_{(m-1)}a^{(m-1)} + b_{(m-2)}a^{(m-2)} + \ldots + b_2a^2 + b_1a + b_0 : b_i \in (0, 1) \quad (3.1)
\]

As the coefficients of the polynomial are 1 and 0, the elements of the finite field can be represented as a string of bits. It should be noted that the elements of the field are reduced modulo some irreducible polynomial and the coefficients are reduced modulo 2.

Addition and multiplication in polynomial representation can be defined as follows:

- Addition of two elements is simply XORing the coefficients of the two elements.
- Multiplication of two elements is performed in the same manner as multiplying two polynomials except in the case of finite fields, the coefficients are reduced modulo 2 and the result is reduced modulo some irreducible polynomial.

**Normal Basis Representation** Consider a \( GF(2^m) \) with \( 2^m \) elements. Let \( \alpha \) be the element of this field such that the \( m \) elements represented by Equation (3.2) are linearly independent. Then equation (3.2) forms the normal basis for the said galois field.

\[
N = \alpha, \alpha^2, \alpha^2, \ldots, \alpha^{2^{m-1}} \quad (3.2)
\]

For such a normal basis, an element in the finite field is then represented by the following equation:

\[
a_0\alpha^0 + a_1\alpha^1 + a_2\alpha^2 + \ldots + a_{m-2}\alpha^{2^{m-2}} + a_{m-1}\alpha^{2^{m-1}} \quad (3.3)
\]

Addition and multiplication in normal basis representation can be defined as follows:
• Addition of two elements is similar to polynomial representation \( i.e. \) XORing the coefficients of the two elements.

• Multiplication of two elements is complex as compared to multiplying two polynomials. The complexity of this multiplication can be reduced by using a class of normal basis known as gaussian normal basis. This multiplication will be explained in section 3.2 \( i.e. \) overview of the multiplier.

• Squaring in normal basis is simply a right rotate of the coefficients of the element of a finite field.

**Elliptic Curves defined over \( GF(2^m) \)**

Elliptic curves in galois fields can be defined by the following equation:

\[
y^2 + xy = x^3 + ax^2 + b
\]  
\[ (3.4) \]

Such an elliptic curve can be formed by choosing elements \( a \) and \( b \) within \( GF(2^m) \) with \( b \neq 0 \). Points \( (x, y) \) \( (x, y \in GF(2^m)) \) satisfy the elliptic curve equation over \( GF(2^m) \). The point at infinity, denoted by \( O \) and the set of solutions \( (x, y) \) form a finite abelian group. Apart from equation 3.4, there are a number of ways in which elliptic curves can be defined and these definitions can be found in any linear algebra textbook.

**Mathematical operations on elliptic curves** The basic elliptic curve operations pertinent to this thesis are defined.

• Addition: Addition of two distinct points \( A \) and \( B \) of an elliptic curve is defined as \( A + B = C \). A line is drawn through points \( A \) and \( B \). This line then intersects point \( -C \) on the curve which is reflected along the x-axis to find the sum \( C \). This is represented graphically in Figure 3.2.

• Doubling: Doubling a point \( A \) is defined as \( 2A = C \). A line tangent to point \( A \) intersects the curve at \( -C \) which is reflected along the x-axis to get \( C \). This is shown graphically in Figure 3.3.

• Scalar Multiplication: Elliptic curve groups do not contain a multiplication operation. Instead a scalar product \( kP \) is defined which is accomplished by adding the point \( P \), \( k \) times.
3.2.2 Overview of the multiplier

The block diagram of this multiplier is shown in Figure 3.4.

The multiplier can be best explained by the following equations. Let $A, B, C$ and $D \in GF(2^m)$ where $m$ is the number of bits needed to represent each element in $GF(2^m)$. Then the product $C$ can be represented as

$$C_{j+1} = C_j^{2^d} XORD(A_j, B_j) \quad (3.5)$$

where $D(A_j, B_j)$ represents an ANDing operation.

$$A_{j+1} = A_j^{2^d} \quad (3.6)$$

$$B_{j+1} = B_j^{2^d} \quad (3.7)$$

where $A_{j+1}$ and $B_{j+1}$ are $d$-fold right cyclic shift operators.
Figure 3.4: Digit-level gaussian normal basis multiplier with parallel output \( DLGM_p \) (adapted from [44]).

The \( DLGM_p \) shown in Figure 3.4 contains three registers \( A, B \) and \( C \). Registers \( A \) and \( B \) store the multiplicand and the multiplier and the register \( C \) stores the output. Block \( P \) consists of XOR gates and manipulates \( A \) in a manner that it can be used for the ANDing operation of equation 3.5. Blocks \( J \) and \( J' \) are used for the ANDing operation of equation 3.5. \( GF(2^m) \) adder consist of an array of XOR gates that implement Equation 3.5 and CS blocks represent the logic needed to implement cyclic shifts for \( A, B \) and \( C \). In the block diagram, \( q \) represents the number of clock cycles required for multiplication, \( d \) represents the number of bits in each digit, \( 1 \leq d \leq m \) and \( r \) is a number between 0 and \( (d - 1) \) such that \( m = (qd - r) \). Blocks \( J \) and \( J' \) are similar but for the fact that \( J' \) is controlled by signal \( q \) and its output is zero at the end of \( (q - 1) \) clock cycles. To understand the architecture of \( DLGM_p \), a multiplier with \( d = 2 \) and \( r = 1 \) for type 4 GNB over \( GF(2^m) \) is illustrated in Figure 3.5.

As can be seen from Figure 3.4 and Figure 3.5, the main components of the multiplier are registers, AND gates and XOR gates. These components will be used from the standard cell library to implement the multiplier.
Figure 3.5: The type 4 $DLGM_p$ over $GF(2^7)(d = 2, r = 1)$ (adapted from [44]).
Chapter 4

Results and Analysis

The first section of this chapter discusses and analyzes the results of the subthreshold circuits in the standard cell library. The next section discusses the functionality of the gaussian normal basis multiplier and gives an insight into the effectiveness of subthreshold implementation of the multiplier against power analysis attacks.

4.1 Standard Cell Libraries

This section explains the results obtained for the standard cell library in subthreshold. All the gates have been designed for a noise margin low \((NM_L)\) of 10% of the supply voltage and noise margin high \((NM_H)\) of 90% of the supply voltage.

4.1.1 INVERTER

**Operating Voltage:** A seven stage ring oscillator is used as a test circuit to identify the inverter characteristics in the subthreshold domain. The inverter operates at a \(V_{dd,limit}\) of 60mV. The \(V_{dd,limit}\) is the lowest supply voltage at which a circuit can operate.

**Aspect Ratios:** The optimal aspect ratio for the worst case and nominal case are identified for the inverter. Optimal aspect ratio is the ratio of the pMOS width to the nMOS width at which the current flowing through the pMOS is equal to the current flowing through the nMOS. A symmetrical output is observed at optimal aspect ratio.

Graph representing the nominal case aspect ratio is shown in Figure 4.1. The width of the pMOS is found such that the output of the ring oscillator is within 10% to 90% of the supply voltage. Maximum pMOS width \((W_{p,max})\) is defined as the width at which the output of the ring oscillator is within 10% of the supply voltage [6]. Minimum pMOS width \((W_{p,min})\) is defined as the width at which the output of the ring oscillator is at least 90% of the supply voltage [6]. As can be seen from the graph, for the nominal case the optimum aspect ratio is \((9/1)\) \(i.e.\) \((W/L)\) for pMOS = \((585 \text{ nm}/65 \text{ nm})\) and \((W/L)\) for nMOS
= (65 nm/65 nm)) and the corresponding supply voltage is 64 mV. The ring oscillator is also simulated for worst case conditions. For \( W_{p,\text{max}} \), the worst case process corner was taken as SF (slow nMOS, fast pMOS) and for \( W_{p,\text{min}} \) pMOS width it was taken as FS (fast nMOS, slow pMOS). These two process corners are sufficient to characterize the behavior of the circuit, as the circuit behavior will be symmetrical at the other two process corners, namely SS (slow nMOS, slow pMOS) and FF (fast nMOS, fast pMOS). Optimum width under worst case conditions is indicated in Figure 4.2.

As can be interpreted from the graph, the aspect ratio for the worst case remains as (9/1) but there is an increase in the minimum operating voltage to 137 mV. To conclude, an aspect ratio of (9/1) is ideal for operating the inverter in subthreshold. So far, the minimum energy point of operation is not yet considered.

**Energy:** To characterize the inverter for minimum energy condition, the ring oscillator was re-simulated with aspect ratios of (2/1) \( (\text{i.e. } (W/L) \text{ for pMOS} = (130 \text{ nm}/65 \text{ nm}) \text{ and } (W/L) \text{ for nMOS} = (65 \text{ nm}/65 \text{ nm})) \text{ and } (5/1) \text{ (i.e. } (W/L) \text{ for pMOS} = (375 \text{ nm}/65 \text{ nm}) \text{ and nMOS} = (65 \text{ nm}/65 \text{ nm}) \text{)
Figure 4.2: Worst case aspect ratio.

and (W/L) for nMOS = (65 nm/65 nm)). The energy characteristics of the ring oscillator at aspect ratio of (2/1) are shown in Figure 4.3 and for aspect ratio (5/1) they are shown in Figure 4.4. The results indicate that leakage energy is dominant in subthreshold and decreases as the supply voltage is increased into the superthreshold region. The point where the leakage and dynamic energy cross is the minimum energy point. The minimum energy point decreases from 195 mV to 190 mV as the aspect ratio is increased from (2/1) to (5/1). Also, the minimum operating voltage, and hence, the power will decrease as the aspect ratio is increased. Thus, we can conclude that if the aspect ratio is further increased to (9/1) the oscillator will operate at the ideal minimum energy point. An aspect ratio of (9/1) is too high especially when the inverter is used as a reference for other circuits.
Figure 4.3: INVERTER energy characteristics; aspect ratio (2/1).
Figure 4.4: INVERTER energy characteristics; aspect ratio (5/1).
**Voltage transfer characteristics:** The voltage transfer characteristics of the inverter for a supply voltage of 140 mV are shown in Figure 4.5. Graphs (a), (b) and (c) indicate the voltage transfer characteristic for aspect ratios (2/1), (5/1) and (9/1). As can be seen from the graphs, the voltage transfer characteristics for the inverter in subthreshold are identical to its superthreshold counterpart. A shift in the midpoint voltage is observed as the aspect ratio is increased from (2/1) to (9/1). For the optimum aspect ratio of (9/1), the midpoint voltage $V_M$ is 74.45 mV which indicates symmetrical output.

![Figure 4.5: INVERTER voltage transfer characteristics.](image)

**Switching activity factor ($\alpha$):** Variation of the minimum energy point with the circuit utility factor $\alpha$ is shown in Figure 4.6. The graph indicates that $V_{\text{min}}$ increases from a value of 162 mV to 196 mV as the value of $\alpha$ decreases from 0.5 to 0.1. This is expected because with an increase in the value of $\alpha$, the transistors in the circuit are utilized more, the circuit is less ideal and the dynamic energy increases. Thus, for a lower minimum energy point, the circuit should be utilized more.
Figure 4.6: Variation of minimum energy point with alpha.
**Frequency and power:** The graph of the inverter frequency for different aspect ratios is shown in Figure 4.7. It can be noted that as the voltage increases, the frequency increases. For the same supply voltage, a lower aspect ratio would give a higher frequency. This is expected as a lower aspect ratio, the resistance is less implying a higher frequency. For an aspect ratio of (2/1) the frequency increases from 33.6 KHz at 130 mV to 14.33 MHz at 400 mV. In comparison, for an aspect ratio of (5/1) the frequency increases from 29.4 KHz to 19.1 MHz as the supply voltage is increased from 100 mV to 400 mV. Thus, for a particular value of \( V_{dd} \), a lower aspect ratio gives a higher frequency.

![Figure 4.7: INVERTER frequency characteristics.](image)

The power characteristics of the inverter are shown in Figure 4.8. As can be seen from the graph the power increases as we move from subthreshold to superthreshold. This is expected because, as the region of operation shifts from subthreshold to superthreshold, the dynamic power increases proportional to the square of the supply voltage. The graph also indicates an increase in the inverter power with an increase in the aspect ratio.
Figure 4.8: INVERTER power characteristics.
4.1.2 Universal Gates

This section explains the design and characteristics of the universal gates, NAND and NOR.

NAND

The NAND gate was simulated using inverter aspect ratios (2/1) and (5/1) as reference.

Energy: The graphs of the total energy in the NAND gate for aspect ratios of (2/1) and (5/1) are shown in Figure 4.9 and Figure 4.10 respectively. From these figures two important observations can be made: 1) The energy of the NAND gate (static and dynamic) has increased with a factor of 1.6 with the sizing. The increase in the aspect ratio increases the load capacitance as well as the circuit delay thereby increasing the static and dynamic energy. 2) The $V_{min}$ reduces from 242 mV to 235 mV as the size of the NAND gate increases from (2/1) and (5/1). This is expected as the optimal aspect ratio for the INVERTER is (9/1). As the aspect ratio increases closer to the reference value of (9/1) the minimum energy point will reduce.
Figure 4.9: NAND energy characteristics: aspect ratio (2/1).
Figure 4.10: NAND energy characteristics: aspect ratio (5/1).
**Frequency and power:** The frequency characteristics for the NAND gate are shown in the Figure 4.11. As expected the frequency of the NAND gate reduces as the aspect ratio is increased. For an aspect ratio of (2/1), the NAND frequency increases from 25.8 KHz to 8.84 MHz as the supply voltage is increased from 140 mV to 400 mV. For the aspect ratio of (5/1) the values are 21.4 KHz and 7.11 MHz respectively. For higher frequency, a low aspect ratio is required but at this aspect ratio the circuit does not work at the lowest minimum energy point. Thus, the operating frequency is a compromise between frequency and energy.

![NAND frequency comparison graph](image)

Figure 4.11: NAND frequency comparison.

The power characteristics of the NAND gate are shown in Figure 4.12. As expected, the power of the NAND gate increases as the supply voltage is increased. It also increases with an increase in the aspect ratio.
Figure 4.12: NAND power comparison.
NOR

Inverter aspect ratios (2/1) and (5/1) were used as a reference for the NOR gate.

Energy:  The energy characteristics for aspect ratio (2/1) and aspect ratio (5/1) are shown in Figure 4.13 and Figure 4.14 respectively. Similar to the NAND gate and the INVERTER, the $V_{\text{min}}$ for the NOR gate reduces from 226 mV to 196 mV as the aspect ratio is increased from (2/1) and (5/1).

![Figure 4.13: NOR energy characteristics: aspect ratio (2/1).](image-url)
Figure 4.14: NOR energy characteristics: aspect ratio (5/1).
**Frequency and power:** For the NOR gate, the frequency values for an aspect ratio of (2/1) are 26.1 KHz and 6.41 MHz for supply voltage of 140 mV and 400 mV respectively. The values for the aspect ratio of (5/1) are 28.7 KHz and 4.76 MHz respectively. The frequency characteristics of the NOR gate is shown in figure 4.15. For the NOR gate too, the power increases as 1) the supply voltage is increased and 2) as the aspect ratio is increased. The power characteristics of the NOR gate are shown in Figure 4.16.

![NOR frequency comparison](image-url)

**Figure 4.15:** NOR frequency comparison.
Figure 4.16: NOR power comparison.
4.1.3 XOR and XNOR

This section explains the characteristics of the XOR and XNOR gates.

![XOR gate diagram](image1)

**Figure 4.17: XOR gate.**

![XNOR gate diagram](image2)

**Figure 4.18: XNOR gate.**

The circuit diagrams for the XOR and XNOR gate are shown in Figure 4.17 and Figure 4.18 respectively. For the XOR gate, minimum sizing was used for the pMOS and nMOS transistors. The (W/L) ratio used for both, the pMOS and the nMOS transistors, was (1/1) \( (i.e. \ (65 \text{ nm}/65 \text{ nm})) \). The XOR gate was inverted to form the XNOR gate. Both, the XOR and the XNOR, operate at a \( V_{dd,limit} \) of 100 mV. At 100 mV, the XOR gate operates at a frequency of 37.6 KHz and dissipates 88.1 nW of power. At this voltage, the XNOR gate operates at a frequency of 32 KHz and dissipates 106 nW of power.
Figure 4.19: Frequency comparison between XOR and XNOR gates.
A comparison between the frequency characteristics of the XOR and the XNOR gates is shown in Figure 4.19. As can be seen from the graph, for the same supply voltage, the XOR gate operates at a higher frequency than the XNOR gate. At 100 mV, the XOR gate operates at a frequency of 37.6 KHz, whereas, the XNOR gate operates at a frequency of 32 KHz. The frequency of the XNOR gate is approximately 1.18 times more than the frequency of the XOR gate. Thus, the presence of the inverter in the XNOR gate reduces the frequency of operation when compared to the XOR gate.

The power characteristics of the XOR and the XNOR gates are shown in Figure 4.20. The graph shows that, for the same supply voltage, the XNOR gate dissipates more power when compared to the XOR. At 100 mV, the XNOR gate dissipates 106 nW of power and the XOR gate dissipates 88.1 nW of power. The XNOR gate dissipates 1.2 times more power than the XOR gate. Thus, the presence of the inverter in the XNOR gate increases its power dissipation considerably when compared to the XOR gate.
4.1.4 FLIP-FLOPS

This section explains the characteristics of the D-flip-flop and the D-multiplier flip-flop.

D flip-flop

The minimum supply voltage at which the D flip-flop operates is 200 mV. At this supply voltage, the flip-flop has a power dissipation of 255 nW and a frequency of 0.5 MHz. The set-up time, hold time and clock-to-q delay for the D flip-flop at 200 mV are 1.850 µs, 1.6733 µs and 0.183 µs respectively. The frequency and power characteristics of the D flip-flop are shown in Figure 4.21 and Figure 4.22 respectively.
Figure 4.22: D flip-flop power characteristics.
D-multiplier flip-flop

In comparison, the D-multiplier flip-flop operates at a minimum voltage of 229 mV. At this voltage the power dissipation of this flip-flop is 652 nW and the frequency of operation is 117 KHz. At 229 mV, the set-up time, hold time and clock-to-q delay for the D-multiplier flip-flop are 6.32 µs, 5.99 µs and 1.8 µs respectively. The frequency and power characteristics of this flip flop are shown in Figure 4.23 and Figure 4.24 respectively.

Figure 4.23: D-multiplier flip-flop frequency characteristics.
Figure 4.24: D-multiplier flip-flop power characteristics.
4.1.5 Multiple Input Gates

This section explains the design and characteristics of 2, 3 and 4-input NAND, NOR, AND and OR gates.

NAND gates

This section describes the characteristics of 2, 3 and 4-input NAND gates. Inverter aspect ratio of (5/1) was used as a reference for these gates.

A 2-input NAND gate is shown in Figure 4.25. The width of the pMOS used for this gate is 10 (i.e. 650 nm). The 2-input NAND gate operates at a $V_{dd,limit}$ of 124 mV. At this voltage, the speed of the gate is 115 KHz and the power dissipation is 10.5 nW. Figure 4.26 shows a 3-input NAND gate. A pMOS width of 15 (i.e. 975 nm) was used to design
this gate. This 3-input NAND gate operates at a $V_{dd,limit}$ of 139 mV. At the $V_{dd,limit}$, the gate operates at a frequency of 97 KHz with a power dissipation of 12.36 nW. A 4-input NAND gate is shown in Figure 4.27. A pMOS width of 20 (i.e. 1350 nm) was used for designing this gate. The $V_{dd,limit}$ for the 4-input NAND gate is 156 mV. At this voltage the gate dissipates 23.2 nW of power and operates at a frequency of 81.9 KHz. It should be noted that the length of the pMOS used for all the three gates is 1, i.e. 65 nm. Also, the width and the length used for sizing the nMOS transistors is 1, i.e. 65 nm. As can be concluded from the results, increasing the number of inputs of a NAND gate increases its minimum operating voltage, i.e. $V_{dd,limit}$. An increase in $V_{dd,limit}$ of 17 mV is observed as the number of inputs to the NAND gate are increased from 2 to 4.

A frequency comparison between the 2-input, the 3-input and the 4-input NAND gate is shown in Figure 4.28. As can be seen from the graph, the frequency of operation decreases as the number of inputs to the NAND gate increase. At 160mV, the frequency of operation of the 2-input NAND gate is 148 KHz, the frequency of operation of the 3-input NAND gate is 107 KHz and the frequency of operation of the 4-input NAND gate is 82.4 KHz. Thus, at the same supply voltage, the 2 input NAND gate is 1.8 times faster than the 4 input NAND gate.
Figure 4.28: Frequency comparison between 2, 3 and 4-input NAND gates.
A comparison between the power characteristics of the 2-input, 3-input and 4-input NAND gate is shown in Figure 4.29. The graph shows that power dissipation in a NAND gate increases with increase in the number of inputs. At 160 mV, a 2-input NAND gate dissipates 16.5 nW of power, a 3-input NAND gate dissipates 23.2 nW of power and a 4-input NAND gate dissipates 25.5 nW of power. Thus, for the same supply voltage, the power dissipation of a 4-input NAND gate is 1.54 times more than the power dissipation of a 2-input NAND gate.

![Power comparison between 2, 3 and 4-input NAND gates.](image)

**Figure 4.29:** Power comparison between 2, 3 and 4-input NAND gates.

**NOR gates**

This section discusses the characteristics of 2, 3 and 4-input NOR gates. Inverter aspect ratio of (5/1) was used as a reference for these gates.

The 2-input NOR, 3-input and 4-input NOR gate are shown in Figure 4.30, Figure 4.31 and Figure 4.32 respectively. A (W/L) ratio of (5/1) (i.e. 375 nm/65 nm) was used for sizing the pMOS transistors of these gates. For the 2-input NOR gate, a (W/L) ratio of (2/1) (i.e. 130 nm/65 nm) was used for the nMOS transistors. The nMOS transistors of
the 3-input NOR gate were sized at a \((W/L)\) ratio of \(3/1\) \(i.e.\) \((195 \text{ nm}/65 \text{ nm})\) whereas the 4-input NOR gate nMOS transistors were sized at a \((W/L)\) ratio of \(4/1\) \(i.e.\) \((260 \text{ nm}/65 \text{ nm})\). The 2-input NOR gate operates at a \(V_{dd,\text{limit}}\) of 108 mV. At this voltage, the speed of the gate is 74.6 KHz and the power dissipation is 26.2 nW. The 3-input NOR gate operates at a \(V_{dd,\text{limit}}\) of 124 mV. At the \(V_{dd,\text{limit}}\), the gate operates at a frequency of 12.9 KHz with a power dissipation of 41.98 nW. The \(V_{dd,\text{limit}}\) for the 4-input NOR gate is 137 mV. At this voltage the gate dissipates 48.23 nW of power and operates at a frequency of 13.2 KHz. As can be concluded from the results, increasing the number of inputs of a NOR gate increases its minimum operating voltage, \(i.e.\) \(V_{dd,\text{limit}}\). An increase in \(V_{dd,\text{limit}}\) of 29 mV is observed as the number of inputs of the NOR gate are increased from 2 to 4.
Figure 4.31: 3-input NOR gate.

Figure 4.32: 4-input NOR gate.
Frequency characteristics of the 2-input, the 3-input and the 4-input NOR gate are shown in Figure 4.33. As can be seen from the graph, the frequency of operation decreases as the number of inputs to the NOR gate increase. At 140 mV, the frequency of operation of the 2-input NOR gate is 94.8 KHz, the frequency of operation of the 3-input NOR gate is 15.8 KHz and the frequency of operation of the 4-input NOR gate is 13.9 KHz. Thus, at the same supply voltage, a 2 input NOR gate is faster by a factor of 7 than a 4-input NOR gate.

A comparison between the power characteristics of the 2-input, 3-input and 4-input NOR gate is shown in Figure 4.34. The graphs show that power dissipation in a NOR gate increases with increase in the number of inputs. At 140 mV, a 2-input NOR gate dissipates 43.9 nW of power, a 3-input NOR gate dissipates 46.0 nW of power and a 4-input NOR gate dissipates 49 nW of power. Thus, for the same supply voltage, the power dissipation of a 4-input NOR gate is 1.15 times more than the power dissipation of a 2-input NOR gate.
Figure 4.34: Power comparison between 2, 3 and 4-input NOR gates.
This section discusses the design and characteristics of 2, 3 and 4-input AND gates. The 2, 3 and 4-input NAND gates were inverted to form the 2, 3 and 4-input AND gates. The inverter used was sized at a (W/L) ratio of (5/1) \(\text{(i.e. } 325 \text{ nm/65 nm})\). The sizing of the NAND gates was kept the same. The 2, 3 and 4-input AND gates are shown in Figure 4.35, Figure 4.36 and Figure 4.37 respectively.

The 2-input AND gate operates at a \(V_{dd,\text{limit}}\) of 133 mV. At this voltage, the speed of the gate is 109 KHz and the power dissipation is 67.88 nW. The 3-input AND gate operates at a \(V_{dd,\text{limit}}\) of 149 mV. At the \(V_{dd,\text{limit}}\), the gate operates at a frequency of 75.8 KHz with a power dissipation of 86.77 nW. The \(V_{dd,\text{limit}}\) for the 4-input AND gate is 160 mV. At this voltage the gate dissipates 121.1 nW of power and operates at a frequency of 69.9 KHz. As can be concluded from the results, increasing the number of inputs of a AND gate increases its minimum operating voltage, \(\text{i.e. } V_{dd,\text{limit}}\). An increase in \(V_{dd,\text{limit}}\) of 28 mV is observed as the number of inputs to the AND gate are increased from 2 to 4. When compared to the NAND gates, for the same number of inputs, the AND gates operate at a higher \(V_{dd,\text{limit}}\).
A frequency comparison between the 2-input, the 3-input and the 4-input AND gate is shown in Figure 4.38. As can be seen from the graph, the frequency of operation decreases as the number of inputs to the AND gate increase. At 160 mV, the frequency of operation of the 2-input AND gate is 118 KHz, the frequency of operation of the 3-input AND gate is 77.6 KHz and the frequency of operation of the 4-input AND gate is 69.9 KHz. Thus, at the same supply voltage, the 2-input AND gate is 1.68 times faster than the 4-input AND gate.
Figure 4.38: Frequency comparison between 2, 3 and 4-input AND gates.
The power characteristics of the 2-input, 3-input and 4-input AND gate are shown in Figure 4.39. The graph shows that power dissipation in an AND gate increases with increase in the number of inputs. At 160 mV, a 2-input AND gate dissipates 79.9 nW amounts of power, a 3-input AND gate dissipates 91.9 nW amounts of power and a 4-input AND gate dissipates 121 nW amounts of power. Thus, for the same supply voltage, the power dissipation of a 4-input AND gate is 1.51 times more than the power dissipation of a 2-input AND gate.
OR gates

This section discusses the design and characteristics of 2, 3 and 4-input OR gates. The 2, 3 and 4-input NOR gates were inverted to form the 2, 3 and 4-input OR gates. The inverter used was sized at a aspect ratio of (5/1). The size of the NOR gates was kept the same. The 2, 3 and 4-input OR gates are shown in Figure 4.40, Figure 4.41 and Figure 4.42 respectively.

![Figure 4.40: 2-input OR gate.](image)

![Figure 4.41: 3-input OR gate.](image)

The 2-input OR gate operates at a $V_{dd,limit}$ of 121 mV. At this voltage, the speed of the gate is 38.2 KHz and the power dissipation is 83.2 nW. The 3-input OR gate operates at a $V_{dd,limit}$ of 135 mV. At the $V_{dd,limit}$, the gate operates at a frequency of 32.8 KHz with a power dissipation of 89.3 nW. The $V_{dd,limit}$ for the 4-input OR gate is 153 mV. At this
Figure 4.42: 4-input OR gate.

voltage the gate dissipates 101 nW of power and operates at a frequency of 20.3 KHz. As can be concluded from the results, increasing the number of inputs of a OR gate increases its minimum operating voltage, \( V_{dd,\text{limit}} \). An increase in \( V_{dd,\text{limit}} \) of 32 mV is observed as the number of inputs of the OR gate are increased from 2 to 4. When compared to the NOR gates, for the same number of inputs, the OR gates operate at a higher \( V_{dd,\text{limit}} \).

Frequency characteristics of the 2-input, the 3-input and the 4-input OR gates are shown in Figure 4.43. As can be seen from the graph, the frequency of operation decreases as the number of inputs to the OR gate increase. At 160 mV, the frequency of operation of the 2-input OR gate is 46.4 KHz, the frequency of operation of the 3-input OR gate is 46 Hz and the frequency of operation of the 4-input OR gate is 29.3 KHz. Thus, at the same supply voltage, a 2 input OR gate is faster by a factor of 1.33 when compared to the 4 input OR gate.
Figure 4.43: Frequency comparison between 2, 3 and 4-input OR gates.
Figure 4.44: Power comparison between 2, 3 and 4-input OR gates.
Power characteristics of the 2-input, 3-input and 4-input OR gate are shown in Figure 4.44. The graphs show that power dissipation in a OR gate increases with increase in the number of inputs. At 160 mV, a 2-input OR gate dissipates 101 nW of power, a 3-input OR gate dissipates 116 nW of power and a 4-input OR gate dissipates 136 nW of power. Thus, for the same supply voltage, the power dissipation of a 4-input OR gate is 1.3 times more than the power dissipation of a 2-input OR gate.

The results for multiple input NAND, AND, NOR and OR gates can be summarized as follows:

- The $V_{dd,limit}$ of any gate increases with the increase in the number of inputs.

- For the same supply voltage, the frequency of operation decreases with increase in the number of inputs. Thus, stacking of transistors decreases the speed of operation.

- For the same supply voltage, power dissipated increases with increase in the number of inputs. Thus, stacking of transistors increases power dissipation.

- For the same number of inputs, an AND gate operates at a higher $V_{dd,limit}$, its frequency of operation is lower and its power dissipation is higher when compared to a NAND gate. Similar characteristics can be observed when comparing the OR gate to the NOR gate.
4.1.6 AND-OR and AND-OR-INVERT Gates

This section explains the design and characteristics of AND-OR and AND-OR-Invert gates.

AO21 and AOI21 gates

This section discusses the design and characteristics of the AND-OR-21 (AO21) and the AND-OR-INVERT-21 (AOI21) gates. The difference between the AO21 and AOI21 gates is the presence of an inverter in the AO21 gate. The AO21 and AOI21 gates are shown in Figure 4.46 and Figure 4.45 respectively.

![Figure 4.45: AOI21.](image)

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.45, the pMOS transistors of the AOI21 gate were sized at a (W/L) ratio of (10/1) \((i.e. \ 650 \ nm/65 \ nm)\). The nMOS transistors for inputs A0 and A1 were sized at a (W/L) ratio of (2/1) \((i.e. \ 130 \ nm/65 \ nm)\) and the for the input B0 the (W/L) ratio of the nMOS transistor used was (1/1) \((i.e. \ 65 \ nm/65 \ nm)\). The AOI21 gate was inverted...
to form the AO21 gate. The inverter used in the AO21 gate was sized at an aspect ratio of (5/1). The $V_{dd,\text{limit}}$ for the AOI21 gate is 210 mV. At this voltage the gate dissipates 102 nW of power and operates at a frequency of 131.6 KHz. The $V_{dd,\text{limit}}$ for the AO21 gate is 289 mV. At this voltage the gate dissipates 113.7 nW of power and operates at a frequency of 46.1 KHz.

A comparison between the frequency characteristics of the AO21 and the AOI21 gates is shown in Figure 4.47. As can be seen from the graph, for the same supply voltage, the AOI21 gate operates at a higher frequency than the AO21 gate. At 290 mV, the AOI gate operates at a frequency of 132 KHz, whereas, the AO21 gate operates at a frequency of 94.7 KHz. The frequency of the AOI21 gate is approximately 1.4 times more than the frequency of the AO21 gate. Thus, the presence of the inverter in the AO21 gate reduces its the frequency of operation when compared to the AOI21 gate.
Figure 4.47: Frequency comparison between AO21 and AOI21 gates.
The power characteristics of the AOI21 and AO21 gates are shown in Figure 4.48. The graph shows that, for the same supply voltage, the AO21 gate dissipates more power when compared to the AOI21 gate. At 290 mV, the AO21 gate dissipates 279 nW of power and the AOI21 gate dissipates 117 nW of power. The AO21 gate dissipates 2.3 times more power than the AOI21 gate. Thus, the presence of the inverter in the AO21 gate increases its power dissipation considerably when compared to the AOI21 gate.

**AO22 and AOI22 gates**

This section discusses the design and characteristics of the AND-OR-22 (AO22) and the AND-OR-INVERT-22 (AOI22) gates. The difference between the AO22 and AOI22 gates is the presence of an inverter in the AO22 gate. The AO22 and AOI22 gates are shown in Figure 4.49 and Figure 4.50 respectively.

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.50, the pMOS transistors of the AOI22 gate were sized at a (W/L) ratio of (10/1) \( (i.e. \ 650 \text{ nm}/65 \text{ nm}) \). The nMOS transistors for this gate were sized at a
(W/L) ratio of (2/1) \(i.e.\) (130 nm/65 nm). The AOI22 gate was inverted to form the AO22 gate. The inverter used in the AO22 gate was sized at an aspect ratio of (5/1). The \(V_{dd,\text{limit}}\) for the AOI22 gate is 210 mV. At this voltage the gate dissipates 42.7 nW of power and operates at a frequency of 38.3 KHz. The \(V_{dd,\text{limit}}\) for the AO22 gate is 218 mV. At this voltage, the gate dissipates 104.7 nW of power and operates at a frequency of 37.7 KHz.
Figure 4.50: AOI22.
Figure 4.51: Frequency comparison between AO22 and AOI22 gates.

The frequency characteristics of the AO22 and the AOI22 gates are shown in Figure 4.51. As can be seen from the graph, for the same supply voltage, the AOI22 gate operates at a higher frequency than the AO22 gate. At 220 mV, the AOI22 gate operates at a frequency of 39.5 KHz, whereas, the AO22 gate operates at a frequency of 37.9 KHz. The presence of the inverter in the AO22 gate reduces the frequency of operation when compared to the AOI22 gate.

A comparison between the power characteristics of the AOI22 and AO22 gates is shown in Figure 4.52. The graph shows that, for the same supply voltage, the AO22 gate dissipates more power when compared to the AOI22. At 220 mV, the AO21 gate dissipates 105 nW of power and the AOI21 gate dissipates 44.8 nW of power. The AO22 gate dissipates approximately 2.3 times more power than the AOI22 gate. The increase in power dissipation in the AO22 gate, when compared to the AOI22 gate, is due to the presence of the inverter in the AO22 gate.
Figure 4.52: Power comparison between AO22 and AOI22 gates.
AO32 and AOI32 gates

Design and characteristics of the AND-OR-32 (AO32) and the AND-OR-INVERT-32 (AOI32) gates are discussed in this section. The difference between the AO32 and AOI32 gates is the presence of an inverter in the AO32 gate. The AO32 and AOI32 gates are shown in Figure 4.53 and Figure 4.54 respectively.

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.54, the pMOS transistors of the AOI32 gate were sized at a (W/L) ratio of (10/1) (i.e. (650 nm/65 nm)), the 2 series nMOS transistors for this gate were sized at a (W/L) ratio of (2/1) (i.e. (130 nm/65 nm)) and the 3 series nMOS transistors were sized at a (W/L) ratio of (3/1) (i.e. (195 nm/65 nm)). The AOI32 gate was inverted to form the AO32 gate. The inverter used in the AO32 gate was sized at an aspect ratio of (5/1). The $V_{dd,limit}$ for the AOI32 gate is 227 mV. At this voltage the gate dissipates 38.6 nW of power and operates at a frequency of 108 KHz. The $V_{dd,limit}$ for the AO32 gate is 235 mV. At this voltage, the gate dissipates 114 nW of power and operates at a frequency of 80.1 KHz.

A comparison between the frequency characteristics of the AO32 and the AOI32 gates are shown in Figure 4.55. As can be seen from the graph, for the same supply voltage, the AOI32 gate operates at a higher frequency than the AO22 gate. At 240 mV, the AOI32 gate operates at a frequency of 112 KHz, whereas, the AO32 gate operates at a frequency of 84.1 KHz. The presence of the inverter in the AO32 gate reduces the frequency of operation.
when compared to the AOI32 gate.
Figure 4.55: Frequency comparison between AO32 and AOI32 gates.
The power characteristics of the AOI32 and AO32 gates are shown in Figure 4.56. The graph shows that, for the same supply voltage, the AO32 gate dissipates more power when compared to the AOI32. At 240 mV, the AO32 gate dissipates 120 nW of power and the AOI32 gate dissipates 47.7 nW of power. The AO32 gate dissipates 2.5 times more power than the AOI32 gate. Thus, the presence of the inverter in the AO32 gate increases its power dissipation considerably when compared to the AOI32 gate.
AO221 and AOI221 gates

This section discusses the design and characteristics of the AND-OR-221 (AO221) and the AND-OR-INVERT-221 (AOI221) gates. The difference between the AO221 and AOI221 gates is the presence of an inverter in the AO221 gate. The AO221 and AOI221 gates are shown in Figure 4.57 and Figure 4.58 respectively.

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.58, the pMOS transistors of the AOI221 gate were sized at a (W/L) ratio of (15/1) \( (975 \text{ nm}/65 \text{ nm}) \). The nMOS transistors for inputs A0 and A1 and inputs B0 and B1 were sized at a (W/L) ratio of (2/1) \( (130 \text{ nm}/65 \text{ nm}) \) and the for the input C0 the (W/L) ratio of the nMOS transistor used was (1/1) \( (65 \text{ nm}/65 \text{ nm}) \). The AOI221 gate was inverted to form the AO221 gate. The inverter used in the AO221 gate was sized at an aspect ratio of (5/1). The \( V_{dd,\text{limit}} \) for the AOI221 gate is 289 mV. At this voltage the gate dissipates 284 nW of power and operates at a frequency of 153.3 KHz. The \( V_{dd,\text{limit}} \) for the AO221 gate is 300 mV. At this voltage the gate dissipates 394 nW of power and operates at a frequency of 80.8 KHz.

A comparison between the frequency characteristics of the AO221 and the AOI221 gates is shown in Figure 4.59. As can be seen from the graph, for the same supply voltage, the AOI221 gate operates at a higher frequency than the AO221 gate. At 300 mV, the AOI221 gate operates at a frequency of 167 KHz, whereas, the AO221 gate operates at a frequency of 80.8 KHz. The frequency of the AOI21 gate is approximately 2 times more than the frequency of the AO221 gate. Thus, the presence of the inverter in the AO221 gate reduces the frequency of operation when compared to the AOI221 gate.
Figure 4.58: AOI221.

Figure 4.59: Frequency comparison between AO221 and AOI221 gates.
Figure 4.60: Power comparison between AO221 and AOI221 gates.

The power characteristics of the AOI221 and AO221 gates are shown in Figure 4.60. The graph shows that, for the same supply voltage, the AO221 gate dissipates more power when compared to the AOI221. At 300 mV, the AO221 gate dissipates 394 nW of power and the AOI21 gate dissipates 314 nW of power. The AO221 gate dissipates approximately 1.3 times more power than the AOI221 gate. Thus, the presence of the inverter in the AO221 gate increases its power dissipation considerably when compared to the AOI221 gate.
AO321 and AOI321 gates

Design and characteristics of the AND-OR-321 (AO32) and the AND-OR-INVERT-321 (AOI32) gates are discussed in this section. The difference between the AO321 and AOI321 gates is the presence of an inverter in the AO321 gate. The AO321 and AOI321 gates are shown in Figure 4.61 and Figure 4.62 respectively.

![Figure 4.61: AO321.](image)

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.54, the pMOS transistors of the AOI321 gate were sized at a (W/L) ratio of (15/1) (i.e. (975 nm/65 nm)), the nMOS transistor for input C0 was sized at a (W/L) ratio of (1/1) (i.e. (65 nm/65 nm)), the 2 series nMOS transistors were sized at a (W/L) ratio of (2/1) (i.e. (130 nm/65 nm)) and the 3 series nMOS transistors were sized at a (W/L) ratio of 3/1 (i.e. (195 nm/65 nm)). The AOI321 gate was inverted to form the AO321 gate. The inverter used in the AO321 gate was sized at an aspect ratio of (5/1). The $V_{dd,limit}$ for the AOI321 gate is 278 mV. At this voltage the gate dissipates 111 nW of power and operates at a frequency of 297 KHz. The $V_{dd,limit}$ for the AO321 gate is 290 mV. At this voltage, the gate dissipates 284 nW of power and operates at a frequency of 218 KHz.

A comparison between the frequency characteristics of the AO321 and the AOI321 gates is shown in Figure 4.63. As can be seen from the graph, for the same supply voltage, the AOI321 gate operates at a higher frequency than the AO221 gate. At 290 mV, the AOI321 gate operates at a frequency of 312 KHz, whereas, the AO321 gate operates at a frequency of 218 KHz. The frequency of the AOI21 gate is approximately 1.4 times more...
than the frequency of the AO221 gate. The presence of the inverter in the AO321 gate reduces the frequency of operation when compared to the AOI321 gate.
Figure 4.63: Frequency comparison between AO321 and AOI321 gates.
The power characteristics of the AOI321 and AO321 gates are shown in Figure 4.64. The graph shows that, for the same supply voltage, the AO321 gate dissipates more power when compared to the AOI321. At 300 mV, the AO321 gate dissipates 284 nW of power and the AOI321 gate dissipates 125 nW of power. The AO321 gate dissipates 2.2 times more power than the AOI321 gate. Thus, the presence of the inverter in the AO321 gate increases its power dissipation considerably when compared to the AOI321 gate.
4.1.7 OR-AND and OR-AND-INVERT Gates

This section explains the design and characteristics of the OR-AND and OR-AND-Invert gates.

OA21 and OAI21 gates

This section discusses the design and characteristics of the OR-AND-21 (OA21) and the OR-AND-INVERT-21 (OAI21) gates. The difference between the OA21 and OAI21 gates is the presence of an inverter in the OA21 gate. The OA21 and OAI21 gates are shown in Figure 4.65 and Figure 4.65 respectively.

![Figure 4.65: OA21.](image)

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.66, the 2 pMOS series transistors of the OAI21 gate were sized at a (W/L) ratio of (10/1) (i.e. (650 nm/65 nm)) and the pMOS transistor connected to input B0 was sized at a (W/L) ratio of (5/1) (i.e. (375 nm/65 nm)). The nMOS transistors were sized at a (W/L) ratio of (2/1) (i.e. (130 nm/65 nm)). The OAI21 gate was inverted to form the OA21 gate. The inverter used in the OA21 gate was sized at an aspect ratio of (5/1).

The $V_{dd,limit}$ for the OAI21 gate is 210 mV. At this voltage the gate dissipates 89.97 nW of power and operates at a frequency of 47.4 KHz. The $V_{dd,limit}$ for the OA21 gate is 219 mV. At this voltage the gate dissipates 31.10 nW of power and operates at a frequency of 42 KHz.
Figure 4.66: OA121.
A comparison between the frequency characteristics of the OA21 and the OAI21 gates is shown in Figure 4.67. As can be seen from the graph, for the same supply voltage, the OAI21 gate operates at a higher frequency than the OA21 gate. At 220 mV, the OAI gate operates at a frequency of 49.9 KHz, whereas, the OA21 gate operates at a frequency of 52.2 KHz. The frequency of the OAI21 gate is approximately 1.1 times more than the frequency of the OA21 gate. Thus, the presence of the inverter in the OA21 gate reduces its frequency of operation when compared to the OAI21 gate.

The power characteristics of the OAI21 and OA21 gates are shown in Figure 4.68. The graph shows that, for the same supply voltage, the OA21 gate dissipates more power when compared to the OAI21. At 220 mV, the OA21 gate dissipates 90 nW of power and the OAI21 gate dissipates 36.6 nW of power. The OA21 gate dissipates 2.44 times more power than the OAI21 gate. Thus, the presence of the inverter in the OA21 gate increases its
power dissipation considerably when compared to the OAI21 gate.
OA32 and OAI32 gates

This section discusses the design and characteristics of the OR-AND-21 (OA32) and the OR-AND-INVERT-32 (OAI32) gates. The difference between the OA32 and OAI32 gates is the presence of an inverter in the OA32 gate. The OA32 and OAI32 gates are shown in Figure 4.69 and Figure 4.69 respectively.

An inverter aspect ratio of (5/1) was used as a reference for sizing these gates. As can be seen from Figure 4.70, the 2 pMOS series transistors of the OAI32 gate were sized at a (W/L) ratio of (10/1) (i.e. (650 nm/65 nm)) and the 3 pMOS series transistors were sized at a (W/L) ratio of (15/1) (i.e. (1025 nm/65 nm)). The nMOS transistors were sized at a (W/L) ratio of (2/1) (i.e. (130nm/65nm)). The OAI32 gate was inverted to form the OA32 gate. The inverter used in the OA32 gate was sized at an aspect ratio of (5/1). The $V_{dd,limit}$ for the OAI32 gate is 220 mV. At this voltage the gate dissipates 35.3 nW of power and operates at a frequency of 66.4 KHz. The $V_{dd,limit}$ for the OA32 gate is 255 mV. At this voltage the gate dissipates 165 nW of power and operates at a frequency of 37.4 KHz.
Figure 4.70: OAI32.
Figure 4.71: Frequency comparison between OA32 and OAI32 gates.
The frequency characteristics of the OA32 and the OAI32 gates is shown in Figure 4.71. As can be seen from the graph, for the same supply voltage, the OAI32 gate operates at a higher frequency than the OA32 gate. At 260 mV, the OAI32 gate operates at a frequency of 51 KHz, whereas, the OA32 gate operates at a frequency of 38.7 KHz. The frequency of the OAI32 gate is approximately 1.32 times more than the frequency of the OA32 gate. Thus, the presence of the inverter in the OA32 gate reduces its frequency of operation when compared to the OAI32 gate.

Figure 4.72: Power comparison between OA32 and OAI32 gates.

The power characteristics of the OAI32 and OA32 gates are shown in Figure 4.72. The graph shows that, for the same supply voltage, the OA21 gate dissipates more power when compared to the OAI32. At 260 mV, the OA32 gate dissipates 185 nW of power and the OAI32 gate dissipates 60 nW of power. The OA32 gate dissipates approximately 3 times more power than the OAI32 gate. Thus, the presence of the inverter in the OA32 gate increases its power dissipation considerably when compared to the OAI32 gate.
4.1.8 NOR0211

This section explains the design and characteristics for the NOR0211 gate.

The circuit diagram for the NOR0211 gate is shown in Figure 4.73. As can be seen from the figure, the NOR0211 gate is a 2-input NAND gate with one of its inputs inverted. A (W/L) ratio of (10/1) (i.e. (650 nm/65 nm)) was used for sizing the pMOS transistors of the NAND gate. The nMOS transistors of the NAND gate were sized at a (W/L) ratio of (1/1) (i.e. (65 nm/65 nm)). The input A1 was applied to an inverter sized at an aspect ratio of (5/1). The NOR0211 operates at a $V_{dd,\text{limit}}$ of 260 mV. At this voltage the frequency of operation of the gate is 98.4 KHz and it dissipates 0.102 nW of power.

The frequency characteristics for the NOR0211 gate are shown in the Figure 4.74. As can be seen from the graph, the frequency of the NOR0211 gate increases as the power supply is increased from 260 mV to 400 mV. The frequency of the gate at 400 mV, increases by a factor of 2.32 when compared to the frequency of the gate at 260 mV.
Figure 4.74: NOR0211 frequency characteristics.
The power characteristics for the NOR0211 gate are shown in the Figure 4.75. As can be seen from the graph, the power of the NOR0211 gate increases as the power supply is increased from 260 mV to 400 mV. The power of the gate at 400 mV, increases by a factor of 3.08 when compared to the power of the gate at 260 mV.
4.1.9 Summary of Standard Cell Library

The results for all the combinational circuits can be best summarized by Table 4.1. The \( V_{dd\text{limit}} \) represents the minimum supply voltage at which the circuit can operate. The contamination delay and propagation delay of the gates, measured at the \( V_{dd\text{limit}} \), are stated in the table. The propagation delay stated in Table 4.1 is the sum of the high-to-low propagation delay, \( t_{pHL} \), and the low-to-high propagation delay, \( t_{pLH} \).

The characteristics of the sequential circuits of the standard cell library are shown in Table 4.2. The \( V_{dd\text{limit}} \) represents the minimum supply voltage at which the circuit can operate. The clock-to-q delay, setup time and hold time of the sequential circuits, measured at the \( V_{dd\text{limit}} \), are stated in the table.

Table 4.3 lists the frequency, power and delay comparison for all the standard cell library gates. AO221 has the highest \( V_{dd\text{limit}} \) of 300 mV. The frequency of operation and power mentioned in the table are for a voltage of 300 mV. The values of high-to-low propagation delay, \( t_{pHL} \), low-to-high propagation delay, \( t_{pLH} \), and contamination delay are also stated at 300 mV. The following equation was used to calculate the frequency of operation of a standard cell:

\[
Frequency = \frac{1}{t_{pHL} + t_{pLH}} \quad (4.1)
\]

where \( t_{pHL} \) is the high-to-low propagation delay and \( t_{pLH} \) is the low-to-high propagation delay.
Table 4.1: Standard cell library characteristics: combinational circuits.

<table>
<thead>
<tr>
<th>Cell</th>
<th>( V_{ddlimit} )</th>
<th>Propagation delay @ ( V_{ddlimit} )</th>
<th>Contamination delay @ ( V_{ddlimit} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVERTER</td>
<td>60 mV</td>
<td>29.76 ( \mu s )</td>
<td>0.00067 ( \mu s )</td>
</tr>
<tr>
<td>NAND2</td>
<td>124 mV</td>
<td>6.76 ( \mu s )</td>
<td>0.0092 ( \mu s )</td>
</tr>
<tr>
<td>NAND3</td>
<td>139 mV</td>
<td>9.35 ( \mu s )</td>
<td>0.0131 ( \mu s )</td>
</tr>
<tr>
<td>NAND4</td>
<td>156 mV</td>
<td>12.1 ( \mu s )</td>
<td>0.0194 ( \mu s )</td>
</tr>
<tr>
<td>AND2</td>
<td>133 mV</td>
<td>8.4 ( \mu s )</td>
<td>0.0102 ( \mu s )</td>
</tr>
<tr>
<td>AND3</td>
<td>149 mV</td>
<td>12.9 ( \mu s )</td>
<td>0.0206 ( \mu s )</td>
</tr>
<tr>
<td>AND4</td>
<td>160 mV</td>
<td>14.3 ( \mu s )</td>
<td>0.0243 ( \mu s )</td>
</tr>
<tr>
<td>NOR2</td>
<td>108 mV</td>
<td>7.5 ( \mu s )</td>
<td>0.0127 ( \mu s )</td>
</tr>
<tr>
<td>NOR3</td>
<td>124 mV</td>
<td>11.3 ( \mu s )</td>
<td>0.0196 ( \mu s )</td>
</tr>
<tr>
<td>NOR4</td>
<td>137 mV</td>
<td>13.9 ( \mu s )</td>
<td>0.022 ( \mu s )</td>
</tr>
<tr>
<td>OR2</td>
<td>121 mV</td>
<td>8.16 ( \mu s )</td>
<td>0.0216 ( \mu s )</td>
</tr>
<tr>
<td>OR3</td>
<td>135 mV</td>
<td>13.7 ( \mu s )</td>
<td>0.0217 ( \mu s )</td>
</tr>
<tr>
<td>OR4</td>
<td>153 mV</td>
<td>16.3 ( \mu s )</td>
<td>0.0341 ( \mu s )</td>
</tr>
<tr>
<td>AO21</td>
<td>289 mV</td>
<td>10.6 ( \mu s )</td>
<td>0.0114 ( \mu s )</td>
</tr>
<tr>
<td>AO22</td>
<td>218 mV</td>
<td>26.4 ( \mu s )</td>
<td>0.0475 ( \mu s )</td>
</tr>
<tr>
<td>AO32</td>
<td>235 mV</td>
<td>11.9 ( \mu s )</td>
<td>0.0214 ( \mu s )</td>
</tr>
<tr>
<td>AO221</td>
<td>300 mV</td>
<td>12.4 ( \mu s )</td>
<td>0.021 ( \mu s )</td>
</tr>
<tr>
<td>AO321</td>
<td>290 mV</td>
<td>4.6 ( \mu s )</td>
<td>0.069 ( \mu s )</td>
</tr>
<tr>
<td>AOI21</td>
<td>210 mV</td>
<td>7.57 ( \mu s )</td>
<td>0.0137 ( \mu s )</td>
</tr>
<tr>
<td>AOI22</td>
<td>210 mV</td>
<td>25.3 ( \mu s )</td>
<td>0.0355 ( \mu s )</td>
</tr>
<tr>
<td>AOI32</td>
<td>227 mV</td>
<td>8.96 ( \mu s )</td>
<td>0.0134 ( \mu s )</td>
</tr>
<tr>
<td>AOI221</td>
<td>289 mV</td>
<td>5.98 ( \mu s )</td>
<td>0.0837 ( \mu s )</td>
</tr>
<tr>
<td>AOI321</td>
<td>278 mV</td>
<td>3.2 ( \mu s )</td>
<td>0.0384 ( \mu s )</td>
</tr>
<tr>
<td>OA21</td>
<td>219 mV</td>
<td>20.01 ( \mu s )</td>
<td>0.0276 ( \mu s )</td>
</tr>
<tr>
<td>OA32</td>
<td>255 mV</td>
<td>19.2 ( \mu s )</td>
<td>0.0367 ( \mu s )</td>
</tr>
<tr>
<td>OA21</td>
<td>210 mV</td>
<td>25.9 ( \mu s )</td>
<td>0.02112 ( \mu s )</td>
</tr>
<tr>
<td>OA32</td>
<td>220 mV</td>
<td>19.6 ( \mu s )</td>
<td>0.0226 ( \mu s )</td>
</tr>
<tr>
<td>NOR0211</td>
<td>260 mV</td>
<td>10.2 ( \mu s )</td>
<td>0.0154 ( \mu s )</td>
</tr>
<tr>
<td>XOR</td>
<td>100 mV</td>
<td>21.3 ( \mu s )</td>
<td>0.0145 ( \mu s )</td>
</tr>
<tr>
<td>XNOR</td>
<td>100 mV</td>
<td>26.67 ( \mu s )</td>
<td>0.0159 ( \mu s )</td>
</tr>
</tbody>
</table>

Table 4.2: Standard cell library characteristics: sequential circuits.

<table>
<thead>
<tr>
<th>Cell</th>
<th>( V_{ddlimit} )</th>
<th>Clock-to-q delay @ ( V_{ddlimit} )</th>
<th>Setup time @ ( V_{ddlimit} )</th>
<th>Hold time @ ( V_{ddlimit} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>D flip-flop</td>
<td>200 mV</td>
<td>0.183 ( \mu s )</td>
<td>1.850 ( \mu s )</td>
<td>1.6733 ( \mu s )</td>
</tr>
<tr>
<td>D-multiplier flip-flop</td>
<td>229 mV</td>
<td>1.8 ( \mu s )</td>
<td>6.32 ( \mu s )</td>
<td>5.99 ( \mu s )</td>
</tr>
</tbody>
</table>
Table 4.3: Frequency, power and delay comparison between standard cell library elements at 300 mV.

<table>
<thead>
<tr>
<th>Cell</th>
<th>Frequency @ 300mV</th>
<th>Power @ 300mV</th>
<th>$t_{pLH}$ @ 300mV</th>
<th>$t_{pHL}$ @ 300mV</th>
<th>Contamination delay @ 300 mV</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVERTER</td>
<td>1.63 MHz</td>
<td>0.316 nW</td>
<td>0.302 µs</td>
<td>0.311 µs</td>
<td>0.00017 µs</td>
</tr>
<tr>
<td>NAND2</td>
<td>338 KHz</td>
<td>42.8 nW</td>
<td>1.50 µs</td>
<td>1.458 µs</td>
<td>0.0029 µs</td>
</tr>
<tr>
<td>NAND3</td>
<td>172 KHz</td>
<td>48.8 nW</td>
<td>2.87 µs</td>
<td>2.94 µs</td>
<td>0.0034 µs</td>
</tr>
<tr>
<td>NAND4</td>
<td>139 KHz</td>
<td>57.2 nW</td>
<td>3.49 µs</td>
<td>3.7 µs</td>
<td>0.0061 µs</td>
</tr>
<tr>
<td>AND2</td>
<td>172 KHz</td>
<td>155 nW</td>
<td>2.89 µs</td>
<td>2.92 µs</td>
<td>0.0033 µs</td>
</tr>
<tr>
<td>AND3</td>
<td>127 KHz</td>
<td>184 nW</td>
<td>3.9 µs</td>
<td>3.97 µs</td>
<td>0.0047 µs</td>
</tr>
<tr>
<td>AND4</td>
<td>120 KHz</td>
<td>235 nW</td>
<td>4.11 µs</td>
<td>4.22 µs</td>
<td>0.0051 µs</td>
</tr>
<tr>
<td>NOR2</td>
<td>764 KHz</td>
<td>243 nW</td>
<td>0.68 µs</td>
<td>0.62 µs</td>
<td>0.0062 µs</td>
</tr>
<tr>
<td>NOR3</td>
<td>204 KHz</td>
<td>306 nW</td>
<td>2.5 µs</td>
<td>2.4 µs</td>
<td>0.0067 µs</td>
</tr>
<tr>
<td>NOR4</td>
<td>173 KHz</td>
<td>330 nW</td>
<td>2.92 µs</td>
<td>2.86 µs</td>
<td>0.0079 µs</td>
</tr>
<tr>
<td>OR2</td>
<td>806 KHz</td>
<td>224 nW</td>
<td>1.14 µs</td>
<td>1.10 µs</td>
<td>0.0069 µs</td>
</tr>
<tr>
<td>OR3</td>
<td>116 KHz</td>
<td>256 nW</td>
<td>4.32 µs</td>
<td>4.3 µs</td>
<td>0.0081 µs</td>
</tr>
<tr>
<td>OR4</td>
<td>88.7 KHz</td>
<td>286 nW</td>
<td>5.9 µs</td>
<td>5.3 µs</td>
<td>0.0093 µs</td>
</tr>
<tr>
<td>AO21</td>
<td>102 KHz</td>
<td>306 nW</td>
<td>4.8 µs</td>
<td>5 µs</td>
<td>0.0055 µs</td>
</tr>
<tr>
<td>AO22</td>
<td>85.5 KHz</td>
<td>237 nW</td>
<td>5.3 µs</td>
<td>5.8 µs</td>
<td>0.0067 µs</td>
</tr>
<tr>
<td>AO32</td>
<td>138 KHz</td>
<td>213 nW</td>
<td>3.44 µs</td>
<td>3.8 µs</td>
<td>0.0054 µs</td>
</tr>
<tr>
<td>AO221</td>
<td>80.8 KHz</td>
<td>394 nW</td>
<td>6.05 µs</td>
<td>6.18 µs</td>
<td>0.0071 µs</td>
</tr>
<tr>
<td>AO321</td>
<td>218 KHz</td>
<td>311 nW</td>
<td>2.25 µs</td>
<td>2.33 µs</td>
<td>0.0084 µs</td>
</tr>
<tr>
<td>AOI21</td>
<td>143 KHz</td>
<td>129 nW</td>
<td>3.33 µs</td>
<td>3.63 µs</td>
<td>0.0045 µs</td>
</tr>
<tr>
<td>AOI22</td>
<td>98.1 KHz</td>
<td>102 nW</td>
<td>5.09 µs</td>
<td>5.1 µs</td>
<td>0.0053 µs</td>
</tr>
<tr>
<td>AOI32</td>
<td>161 KHz</td>
<td>125 nW</td>
<td>3.02 µs</td>
<td>3.19 µs</td>
<td>0.0078 µs</td>
</tr>
<tr>
<td>AOI221</td>
<td>167 KHz</td>
<td>314 nW</td>
<td>5.55 µs</td>
<td>5.43 µs</td>
<td>0.0064 µs</td>
</tr>
<tr>
<td>AOI321</td>
<td>312 KHz</td>
<td>138 nW</td>
<td>1.52 µs</td>
<td>1.68 µs</td>
<td>0.0092 µs</td>
</tr>
<tr>
<td>OA21</td>
<td>99.4 KHz</td>
<td>204 nW</td>
<td>5.1 µs</td>
<td>4.906 µs</td>
<td>0.0042 µs</td>
</tr>
<tr>
<td>OA32</td>
<td>61.7 KHz</td>
<td>217 nW</td>
<td>8.2 µs</td>
<td>8 µs</td>
<td>0.0051 µs</td>
</tr>
<tr>
<td>OA121</td>
<td>117 KHz</td>
<td>83.7 nW</td>
<td>4.31 µs</td>
<td>4.23 µs</td>
<td>0.0053 µs</td>
</tr>
<tr>
<td>OA132</td>
<td>140 KHz</td>
<td>89.8 nW</td>
<td>3.58 µs</td>
<td>3.56 µs</td>
<td>0.0059 µs</td>
</tr>
<tr>
<td>NOR0211</td>
<td>98.4 KHz</td>
<td>0.102 nW</td>
<td>2.26 µs</td>
<td>2.23 µs</td>
<td>0.0088 µs</td>
</tr>
<tr>
<td>XOR</td>
<td>46.9 KHz</td>
<td>213 nW</td>
<td>1.12 µs</td>
<td>1.08 µs</td>
<td>0.0016 µs</td>
</tr>
<tr>
<td>XNOR</td>
<td>37.5 KHz</td>
<td>314 nW</td>
<td>1.39 µs</td>
<td>1.32 µs</td>
<td>0.0021 µs</td>
</tr>
<tr>
<td>D flip-flop</td>
<td>798 KHz</td>
<td>914 nW</td>
<td>0.64 µs</td>
<td>0.61 µs</td>
<td>0.0083 µs</td>
</tr>
<tr>
<td>D-multiplier flip-flop</td>
<td>128 KHz</td>
<td>1280 nW</td>
<td>3.93 µs</td>
<td>3.85 µs</td>
<td>0.0088 µs</td>
</tr>
</tbody>
</table>
4.1.10 Process variation

Subthreshold systems are sensitive to process variations. While designing subthreshold circuits these process variations should be accounted and a technique to control these variations should be implemented. For the IBM 65nm technology file used, the process variations for a particular corner are defined by the parameter $\sigma$. The inverter power characteristic for the positive values of $\sigma$ is shown in Figure 4.76 and for the negative values of $\sigma$ is shown in Figure 4.77. An increase in the inverter power is observed for constant $V_{dd}$ as the value of sigma becomes more positive. For example, at 300 mV the power for a value of $\sigma$ of -3 is 9.92e-13 while the power at a $\sigma$ value of 3 is 2.07e-6 almost 2.08e-6 times more. This substantial increase in power is due to an increase in current as the transistor width increases and channel length reduces for a more positive $\sigma$ value.

![Figure 4.76: Inverter power for positive sigma values.](image-url)
Figure 4.77: Inverter power for negative sigma values.
As can be observed from Figure 4.78 and Figure 4.79, the frequency too increases with an increase in $\sigma$ value. For 300 mV, the increase in frequency at $\sigma$ value 3 is $1.36\times10^6$ times the frequency at sigma value -3. As the sigma value becomes more positive, the series resistance and capacitance of the transistor reduce, resulting in an increase in the frequency value for constant $V_{dd}$.

Figure 4.78: Inverter frequency for positive sigma values.
Figure 4.79: INVERTER frequency for negative sigma values.
4.2 Performance Evaluation of Multiplier

This section explains the functionality of the multiplier and discusses the effectiveness of the subthreshold implementation of the multiplier in increasing resistance to power analysis attacks.

4.2.1 Functionality

The functionality of the multiplier can be best explained by comparing the output obtained from the spice file with a MATLAB program. Figure 4.80 and Figure 4.81 represent the output of the subthreshold and superthreshold multiplier respectively.

The MATLAB program for the multiplier and its output are given below.

```matlab
*****PROGRAM*****\ 
Finding minimum polynomial of GF(2,7)
m = 7;
A = gf(2,m);
p1 = minpol(A);
```

Figure 4.80: Subthreshold $DLG_M$ output.
Figure 4.81: Superthreshold $DLGM_p$ output.

\[ p = 2; \ m = 7; \]
\[ a = [0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1]; \ b = [0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1]; \]
\[ \text{notsimple} = \text{gfconv}(a,b,p)\% \ a \times b, \ \text{using} \]
\[ \% \text{high powers of alpha} \]
\[ \text{simple} = \text{gftuple}(\text{notsimple},m,p)\% \text{Highest exp. of alpha is m-1} \]

*****OUTPUT*****

\[ A = \text{GF}(2^7) \ \text{array}. \]
\[ \text{Primitive polynomial} = D^7+D^3+1 \ (137 \ \text{decimal}) \]

Array elements =

\[ 2 \]

\[ pl = \text{GF}(2) \ \text{array}. \]

Array elements =

\[ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \]
notsimple =

0 0 0 0 0 0 0 0 0 0 1 1 1

simple =

1 1 0 0 0 1 1

The “notsimple” output in the program represents the multiplication output in binary and the simple output in the program represents the polynomial multiplication output. The functionality of the multiplier can be easily verified from Figure 4.80, Figure 4.81 and the “simple” output of the MATLAB program.

4.2.2 Effectiveness of the subthreshold operation against power analysis attacks

A simple power analysis example is shown in Figure 4.82. The graphs in the figure represent the supply current trace of the superthreshold multiplier. The lower graph represents the supply current for an input of 0000011 and the upper graph represents the supply current for the input 111111 applied. A change in the current trace is clearly visible for the change in input. Thus an attacker can easily find a correlation between the change in the supply current to the input applied.
Figure 4.82: Simple power analysis.

A = 1111111
B = 0000001

A = 0000011
B = 0000001

Considerable amount of power change is observed
In a differential power analysis the attacker observes thousands of such current (power) traces and using sophisticated statistical methods to find a correlation between the operation performed and the current (power) trace. The supply current graphs for the subthreshold and superthreshold multipliers for 1000 random input combinations are shown in Figure 4.83 and Figure 4.84 respectively.

![Graph showing current traces for 1000 random input combinations at V_{dd} = 0.3V.](image)

Each line in the graph represents supply current for a particular input combination.

Figure 4.83: Current traces for 1000 random input combinations at V_{dd} = 0.3V.

As can be observed from the figures, the supply current of the subthreshold multiplier is 33 times less than that of the superthreshold multiplier. At such low current values, the attacker might need infinitely large current traces to perform the differential power analysis.
Each line in the graph represents supply current for a particular input combination.

Figure 4.84: Current traces for 1000 random input combinations at $V_{dd} = 1.2V$. 
A 7 bit prototype $DLGM_p$ multiplier was designed and simulated for analysis. The multiplier operates at a $V_{dd\text{limit}}$ of 267 mV. At this voltage the power consumption of the multiplier is 4.554 $\mu$W and speed of the multiplier is 65.1 KHz. In comparison, at 1.2 V, i.e. in the superthreshold region, this multiplier operates at a speed of 330 MHz and power consumption of 4.005 mW. Thus, a power saving of is observed for the subthreshold multiplier at the cost of reduction in speed.

![Figure 4.85: Subthreshold and superthreshold multiplier power trace comparison.](image)

The power graphs for the subthreshold and superthreshold multipliers are shown in Figure 4.85. As can be seen from the graph the subthreshold power is very low as compared to the superthreshold case (the graph almost touches the x-axis). At such low power levels it becomes increasingly difficult for the attacker to mount a power analysis attack. Since the attacker does not know that the system is implemented in subthreshold, he might misinterpret such low signal levels as noise. The SNR for the multiplier in subthreshold and superthreshold was calculated. The SNR reduces considerably from 200dB in superthreshold to about 40dB in subthreshold.

For the multiplier operating in the subthreshold region, the signal magnitude becomes comparable to noise. At such low magnitudes it is very difficult for an attacker to correlate
the outputs of the multiplier to the change in inputs. Thus, by operating cryptographic
systems at subthreshold, the difficulty in mounting DPA attacks against them is greatly
increased.
Chapter 5

Conclusions and Future Work

5.1 Conclusions

In this thesis, a 7 bit prototype $DLGM_p$ multiplier is implemented in subthreshold and superthreshold regions of operation. In subthreshold, the multiplier operates at a minimum supply voltage of 267 mV. At this voltage the power consumption of the multiplier is $4.554 \, \mu W$ and speed of the multiplier is 65.1 KHz. In comparison, at 1.2 V, i.e. in the superthreshold region, this multiplier operates at a speed of 330 MHz and power consumption of 4.005 mW. Thus, a significant amount of power saving is observed for the subthreshold multiplier at the cost of reduction in speed. The supply current for subthreshold multiplier is almost negligible when compared to the supply current of the superthreshold multiplier. Also the SNR for the subthreshold multiplier is 40 dB as compared to 200 dB for the superthreshold case. Thus, by operating the multiplier in subthreshold, the signal magnitude becomes comparable to noise. At such low magnitudes the correlation between the outputs of the multiplier to the change in inputs is greatly reduced. Thus, cryptographic systems at subthreshold increase the difficulty in mounting DPA attacks against them.

This research also outlines a basic methodology for design of standard cells in subthreshold. The design of these cells is a compromise between sizing, energy and frequency of operation. The minimum energy point decreases as the aspect ratio is increased but this also reduces the frequency of operation. The lowest minimum energy point is observed for an aspect ratio of $(9/1)$ for the inverter. However such a large sizing is not suitable for circuits which use the inverter as their reference. Therefore for the standard cells designed we have used a sizing of $(5/1)$ to achieve minimum energy and integral performance. For a given aspect ratio, the minimum energy point decreases as the transistor activity factor increases. This is expected because as $\alpha$ increases, the circuit is being utilized more and there is an increase in the dynamic energy at the cost of leakage energy. For high switching activity circuits it is more feasible to operate at the minimum energy point compared to low switching activity circuits. The minimum energy point shifts to a higher level with stacking of transistors as seen in NAND and NOR gates. Therefore stacking of transistors should
be minimal in subthreshold. Subthreshold circuits are considerably affected by process variations and these variations should be considered while designing these circuits.

5.2 Future Work

The prototype multiplier implemented in this work proves that subthreshold circuits can be used to increase resistance against power analysis attacks. This proof of concept can be extended to a standard 163 bit multiplier approved by the NIST. Further, a full chip implementation of a complete ECC system should be produced to take advantage of the key points of this thesis. Subthreshold circuits could be used with other DPA countermeasures to strengthen the resistance against power attacks. The ultimate goal should be to provide a cryptographic system immune to power attacks. Subthreshold circuits are highly sensitive to process variations. Therefore, new design techniques are needed to subside the effects of process variations. Body biasing could be one such technique that can be implemented to increase the robustness of the subthreshold system.
Bibliography


[29] Jae-Joon Kim and Kaushik Roy. Double gate MOSFET subthreshold circuit for ultra-


[33] Ranjith Kumar and Volkan Kursun. Temperature-adaptive energy reduction for ultra-
low power-supply-voltage subthreshold logic circuits. In *IEEE International Confer-


power operation. In *IEEE Computer Society Annual Symposium on VLSI: Emerging 

[36] Siva Narendra, Vivek De, Shekhar Borkar, Dimitri A. Antoniadis, and Anantha P. 
Chandrakasan. Full-chip subthreshold leakage power prediction and reduction tech-
niques for sub-0.18-μm CMOS. *IEEE Journal of Solid-State circuits*, 39(3):501–510, 
March 2004.


[38] Toshinori Numata and Shinichi Takagi. Device design for subthreshold slope and 
threshold voltage control in sub-100-nm fully depleted SOI MOSFETs. *IEEE Trans-


