REALIZATION OF NON-LINEAR SIGNAL PROCESSING BLOCKS, STANDARD FUNCTIONS AND APPLICATION TO CRYPTOGRAPHY

A DISSERTATION

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

MASTER OF TECHNOLOGY
IN
CONTROL & INSTRUMENTATION

Submitted by:

ANKUR SINGH

2K16/C&I/04

Under the supervision of

PROF. PRAGATI KUMAR

DEPARTMENT OF ELECTRICAL ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

JULY, 2018

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, Ankur Singh, Roll No. 2K16/C&I/04 student of M.Tech. (Control & Instrumentation), hereby declare that the Dissertation titled "**Realization of Non-Linear Signal Processing Blocks, Standard Functions and Application to Cryptography**" which is submitted by me to the Department of Electrical Engineering, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship or other similar title or recognition.

Place: Delhi **ANKUR SINGH**
Date:

DEPARTMENT OF ELECTRICAL ENGINEERING

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Dissertation titled "**Realization of Non-Linear Signal Processing Blocks, Standard Functions and Application to Cryptography**" which is submitted by Mr. Ankur Singh, Roll No 2K16/C&I/04 Electrical Engineering Department, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the students under my supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

Date:

PROF. PRAGATI KUMAR

SUPERVISOR

Professor

ABSTRACT

Non-Linear signal processing circuits are used in various streams of engineering such as telecommunication, control system, digital design, biomedical, information security etc. Various types of signal processing methods such as analog or digital are used according to applications and requirements. CMOS non-linear signal processing circuits consume less power whereas bipolar non-linear circuits provide faster response and also provide wide operating range.

In this dissertation linear term generator and higher order non-linear blocks such as squarer generator, cubic generator, power four generator and power five generator blocks have been implemented.

The functions like sine, cosine, exponential, logarithmic, tangent hyperbolic inverse functions and the other two functions viz. Gaussian and sigmoid, which are extensively used in artificial neural network are also implemented in this dissertation. These functions are implemented in current mode since this mode is found to be more advantageous as compared to voltage mode implementation.

The analog implementation of elliptic curve using these non-linear blocks is also presented in this dissertation which can be further used in Cryptography.

ACKNOWLEDGEMENT

First and foremost, I express my deep sense of gratitude to my supervisor, counselor and advisor **Prof. Pragati Kumar**, Professor, department of Electrical Engineering for his constant guidance, support, motivation and encouragement throughout the period this work was carried out. His readiness for consultation at all times, his educative comments, his concern and assistance has been invaluable.

I want to thank **Prof. Madhusudan Singh,** Head of Electrical Department for building this platform and creating such an energetic environment for research work.

I want to thank **Mr. Ajishek Raj** (Research Scholar) for his guidance and support and all the staff of the Non-Linear Signal Processing Lab, Electrical Engineering Department for their fullest cooperation.

I would like to thank my friends and all those who have directly or indirectly helped me in completion of the thesis well in time.

Finally, I wish to thank my parents for their moral support and confidence showed in me to pursue M. Tech at an advanced stage of my academic career.

ANKUR SINGH

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS, ABBREVIATION

V_{GS} – Gate to Source Voltage

V_{SG} – Source to Gate Voltage

I_D – Drain Current

μ_n – Mobility of Electron

μ_p – Mobility of Holes

W/L – Aspect Ratio

I_o, I_p, I_q, I_s, I_a, I_b, I_α – Biasing Current

$+V_{cc}$, V_{DD}, $+V_{EE}$ – Positive Power Supply

$-V_{cc}$, V_{SS}, $-V_{EE}$ – Negative Power Supply

M_i – i^{th} MOSFET

Q_i – i^{th} Bipolar Transistor

V_o – Output Voltage

I_S – Reverse Saturation Current

V_{BE} – Base Emitter Voltage

V_{EB} – Emitter Base Voltage

V_T – Thermal Voltage

V_B – Base Voltage

I_C – Collector Current

I_B – Base Current

I_E – Emitter Current

β_n – Collector-Base Current Gain for npn Transistor

β_p – Collector-Base Current Gain for pnp Transistor

V_{in+} – Positive Input Voltage

V_{in-} – Negative Input Voltage

I_{out} – Output Current

I_{in} – Input Current

V_t – Threshold Voltage of NMOS and PMOS

V_G – Gate Voltage

λ – Process technology parameter

k_n – Transconductance for N-Channel MOSFET

k_p –Transconductance for P-Channel MOSFET

S_i – Aspect Ratio of NMOS and PMOS

A_i – Area of Bipolar Transistor

β –Collector-Base Current Gain for both npn and pnp bipolar transitors

ϕ, ρ, Υ, σ, μ, γ – Ratios of Collector-Base Current Gain

I_t – Counter-Clockwise Collector Current

I_W – Clockwise Collector Current

I_{Dt} – Counter-Clockwise Drain Current

I_{DW}– Clockwise Drain Current

C_{OX} – oxide capacitance

CMOS - Complementary Metal Oxide Semiconductor

CCII – Current Conveyor Second

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

The presented work describes the design and implementation of current-mode non-linear signal processing blocks and their applications in implementation of some non-linear functions like sine, cosine, e^x, Gaussian function, ln(1+x) etc. Lot of research work is going in the field of data security and in this dissertation an attempt has also been made to introduce analog implementation of Elliptic curve which may be used in Cryptography to enhance security.

Because of advances made in CMOS technology there has been a significant reduction in the cost of digital hardware which has led to increased use of digital systems. Digital systems offer several advantages over analog systems but the fact which cannot be ignored is that all signals available in natural world are analog. To match with the fast growing digital part, extensive research has been carried out in the field of non linear signal processing in current mode and voltage but current mode approach was found to have some advantages like higher frequency operating range, more accurate, greater value of slew rate, less consumption of power and better linearity [1].

Before going into the detail of implemented work we will first go through the basic concepts associated with signal processing.

1.2 ANALOG VS DIGITAL SIGNAL PROCESSING

The signal processing operations involved in many applications like communication systems, control systems, instrumentation, biomedical signal processing etc can be implemented in two different ways

1) Analog or continuous time method and
2) Digital or discrete time method.

The analog approach to signal processing was dominant for many years and it use analog circuit element such as resistors, capacitors, transistors, diodes etc. With the advent of digital computer and later microprocessor, the digital signal processing has become dominant now a days. The analog signal processing is based on natural ability of the analog system to solve differential equations that describe a physical system. The solutions are obtained in real time. In contrast digital signal processing relies on numerical calculations. The method may or may not give result in real time. The digital approach has two main advantages over analog approach (1) Flexibility: Same hardware can be used to do various kind of signal processing operation, while in the core of analog signal processing one has to design a system for each kind of operation. (2). Repeatability: The same signal processing operation can be repeated again and again giving same results, while in analog systems there may be parameter variation due to change in temperature or supply voltage [2]. Added to these, digital signal processing has many advantages added to its list like, better noise immunity than analog signals. They are compact and much cheaper than their analog counterpart. Digital signals can be encrypted so that only the intended receiver can decode it. It enables transmission of signals over a long distance and it enables multi-directional transmission simultaneously [3].

Taking these advantages into the account, the designers are forced to look for digital solutions rather than analog in VLSI systems. Even then, analog circuits are fundamentally necessary in many of the today's complex, high performance systems. This is caused by the reality that naturally occurring signals are analog. Practically all signals in the physical world are continuous in both amplitude and time, and hence always analog techniques will be required for

conditioning of such signals before they can be processed by digital processing circuits. Therefore analog circuits act as a bridge between the real world and digital systems. Another important reason for the existence of analog signal processing is the bandwidth, which can be some order of magnitudes higher, if the signal is processed in analog circuits than in digital.

1.3 VOLTAGE MODE, CURRENT MODE AND MIXED MODE SIGNAL PROCESSING

Over the past couple of decades, the area of analog signal processing has been viewed in terms of the dominant variables of the circuit viz. voltage and current. The signal processing of any electronic and electrical circuits where voltages and currents are important variables. The main cause of using voltage and current in signal processing is that the active devices which are operate usually with resistances or conductances [4].

1.3.1 VOLTAGE MODE SIGNAL PROCESSING

In signal processing circuits, there are two main parameters that are mostly considered: either voltage or current. While others are considered as an unwanted parasitic. In the past, voltage has been considered as the main variable in signal processing. Approach in terms of voltages instead of current is very easier and simpler for the designers [4]. The input impedance of voltage mode device is very high, ideally it is infinite, so that there is no loss of signal power. Through this arrangement, it is possible to connect more input terminals parallel with only signal output terminal. The output impedance of the terminals of voltage mode device are ideally zero. Having low output impedance makes it possible to drive heavy load by single output [4]. There are parasitic resistances as well as capacitances present at input terminals of voltage mode circuit, which can affect performance of the circuit. These parasitic also affect output terminals, which is not allowed to drive heavy load at output terminal. The effect of inductances parasitic has not significant meaning in VLSI processing. The main advantage of voltage mode circuits that a single voltage-output terminal could supply more input terminals which are connected parallel.

1.3.2 CURRENT MODE SIGNAL PROCESSING

In current mode signal processing, the dominant variable is current (both input as well as output). The devices used (amplifiers) have very low input impedance, ideally zero and very high output impedance, ideally infinite. As a result, cascading of inputs and outputs with voltage device are not possible. These devices are characterized by very small voltage swings which result in fast speed. Also, the signal processing circuitry becomes simpler and lesser number of components are required (for adding currents no extra amplifiers is needed). Another very important feature of the current mode device is large dynamic range of the input quantity. [5] [6] [7].

1.3.3 MIXED MODE SIGNAL PROCESSING

In this mode of signal processing both current and voltage variables are the integral part of the signal space of the application and help in matching the impedance levels at the input and output side.

1.4 CRYPTOGRAPHY AND NETWORK SECURITY

To ensure the security of network by implementing the security for data we require a technique called Cryptography. Cryptosystems using neural network provide higher security. Neural network is formed of neuronal or activation function along with weights and these functions with weights could be the key or code for our security purpose which could be difficult to estimate. Decryption of messages without having the knowledge of encryption technique used i.e. a hit and trial method falls under Cryptanalysis [8] [9].

Encryption, the process to convert the information which is in plaintext form into incomprehensible text called cipher text or encrypted message. The reverse of it is decryption i.e. breaking out the plaintext from cipher text. Security services provided by protocol layer of communicating open systems gives data integrity, confidentiality, authenticity, and non-repudiation. Major applications of Cryptography are in systems like ATMs, electronic commerce and passwords for computers. Development in World Wide Web has resulted in major use of Cryptography for e-commerce and applications in business [9].

1.5 ORGANISATION OF THE THESIS

In Chapter 2, we have briefly discussed translinear circuit principle and some of the important existing non linear analog blocks and derived functions.

In Chapter 3, the Translinear principle based basic modules used in various approximations have been discussed.

In Chapter 4, some applications of our basic modules are presented as realization of various approximated functions and their applications.

In Chapter 5, the discussion on Elliptic curve along with its properties and along with its analog implementation in Cryptography for network security.

In Chapter 6, Summary of whole thesis is done along with Future scope has been discussed.

REFERENCES

[1] J. Huijsing, R. van de Plassche, W. Sansen (Eds.), "Analog circuit design: Low-noise, low-power, low-voltage, Mixed-mode design with Cad Tools Voltage, Current and Time References," *Kluwer*, 1996, pp. 269-352.

[2] nptel(2018) *analog versus digital signal processing,* Available at: *http://nptel.ac.in/courses/Webcourse-contents/IIT-KANPUR/Digi_Sign_Pro/lecture1/images/node3.html* (Accessed: 5 July 2018).

[3] nptel(2018) *digital system advantages,* Available at: *http://nptel.ac.in/courses/117103064/2* (Accessed: 4 July 2018)

[4] Igor M.,"New Circuit Principle of Integrated Circuits," Part 2: Special Function Blocks for Analog current signal processing, PhD Thesis, Brno University of Technology,2010.

[5] Toumazou C., Lidgey F.J., Haigh D.G. (Eds.), "Analogue IC design: The current-mode approach," *IEE Circuits and Systems Series 2*, Perigrinus Press, 1990

[6] J. W. HASLETT, M. K. N. RAO, "A High Quality Controlled Current Source," *IEEE Trans. Instrumentation and Measurement*, vol. IM-28, No. 2, 1979.

[7] Groza R., M. Cirlugia, "Current mode configurational analog block," *IEEE transaction*,978-1-5090-3748-3,2016.

[8] W. Stallings, Cryptography And Network Security Principles and Practices, *PrenticeHall*,2012.

[9] S.N. Kumar,"Review on Network Security and Cryptography," *International Transaction Of Electrical and Computer Engineers System*, 2015 3 (1),pp1-11.

CHAPTER 2

NON LINEAR BLOCKS AND FUNCTIONS

2.1 INTRODUCTION

Since the presented work deals with analog circuit realization of some non linear functions, it is worthwhile to present a review of the basic building blocks used in the realization of these non-linear functions. The building blocks used are

1. Logarithmic block
2. Exponential block
3. Square rooting block
4. Linear block

Most of these blocks utilize the translinear circuit principle [1] proposed by Gilbert for bipolar transistors or its CMOS version. We first present the TCP (Translinear circuit principle) in the following section.

2.2 TRANSLINEAR PRINCIPLE

A closed loop circuit consisting of even number of transistors and all having their base emitter junction forward biased, along with arranged in such a fashion that half of them having clockwise polarity and half of them having anti-clockwise polarity then the sum of forward biased base emitter junction in clockwise

is equal to forward biased base emitter junction in counter clockwise [1], as shown in Fig 2.1 below.

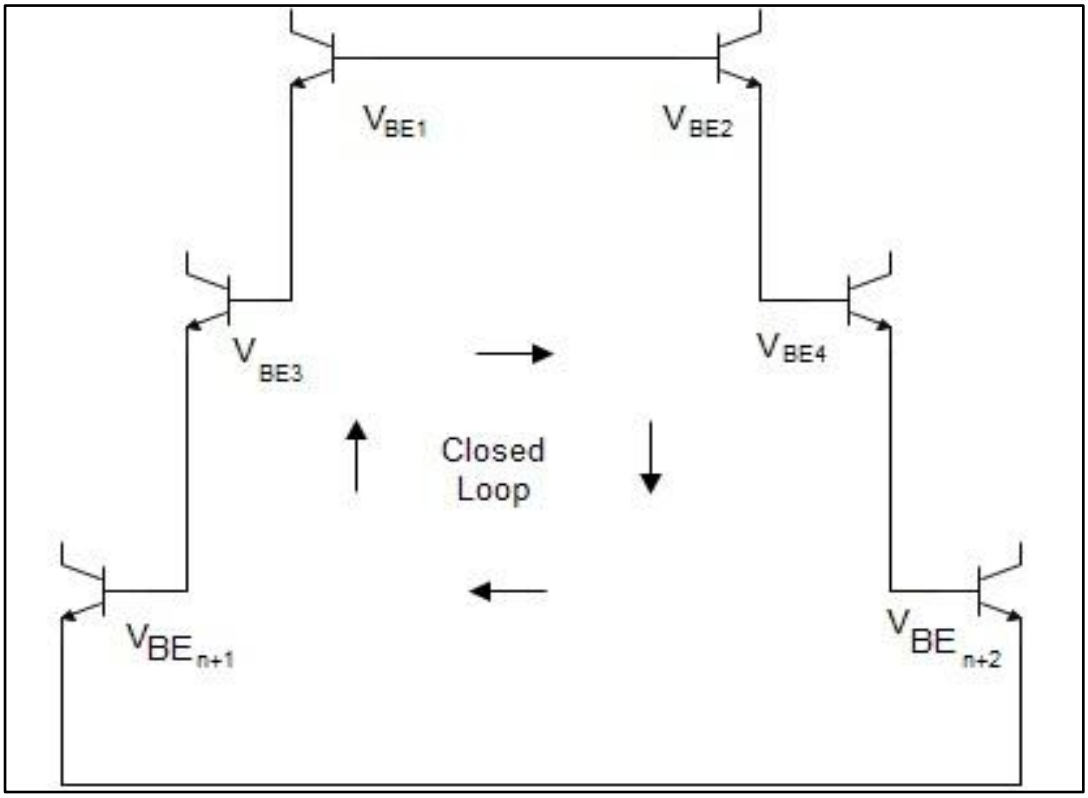

Fig 2.1 Translinear Loop

From above Fig 2.1, it can expressed as,

$$\sum_{t=1}^{n+1} V_{BEt} = \sum_{w=2}^{n+2} V_{BEw} \quad (2.1)$$

Where, left hand side of above equation is sum of voltages in counter clockwise direction and right hand side is sum of voltages in clockwise direction.

Therefore,

$$\prod_{t=1}^{n+1} I_t = \prod_{w=2}^{n+2} I_w \quad (2.2)$$

Since, $V_{BE} = V_T \ln\left(\frac{I_C}{I_S}\right)$

The above relation in equation 2.3 is for translinear loop formed with the help of bipolar transistors. Similar analysis can be done for translinear loop consisting of MOSFETs, in which all transistors are made to operate in saturation region. The relation for such case is given as follow:

$$\sum_{t=1}^{n+1} V_{GSt} = \sum_{w=2}^{n+2} V_{GSw} \quad (2.3)$$

Or,

$$\sum_{t=1}^{n+1} \sqrt{\frac{I_{Dt}}{K_t\left(W/L\right)_t}} = \sum_{w=2}^{n+2} \sqrt{\frac{I_{Dw}}{K_w\left(W/L\right)_w}} \quad (2.4)$$

2.3 TRANSLINEAR BASED CIRCUITS

Among the various analog multiplier circuits that can be used as squarer block and some CMOS based squarer circuits presented in [2] [3] [4] [5] we have analyzed one of the blocks that has been presented in the following section.

2.3.1 SQUARER AND LINEAR BLOCK

The application of the principle of translinear loop is shown in Fig 2.2, which results in scaled squarer and inverted linear term. In the following CMOS circuit the very important parameter is the matching of the transistors with their W/L ratios along with keeping in mind the relationship between electron mobility (μ_n) and hole mobility (μ_p) [5].

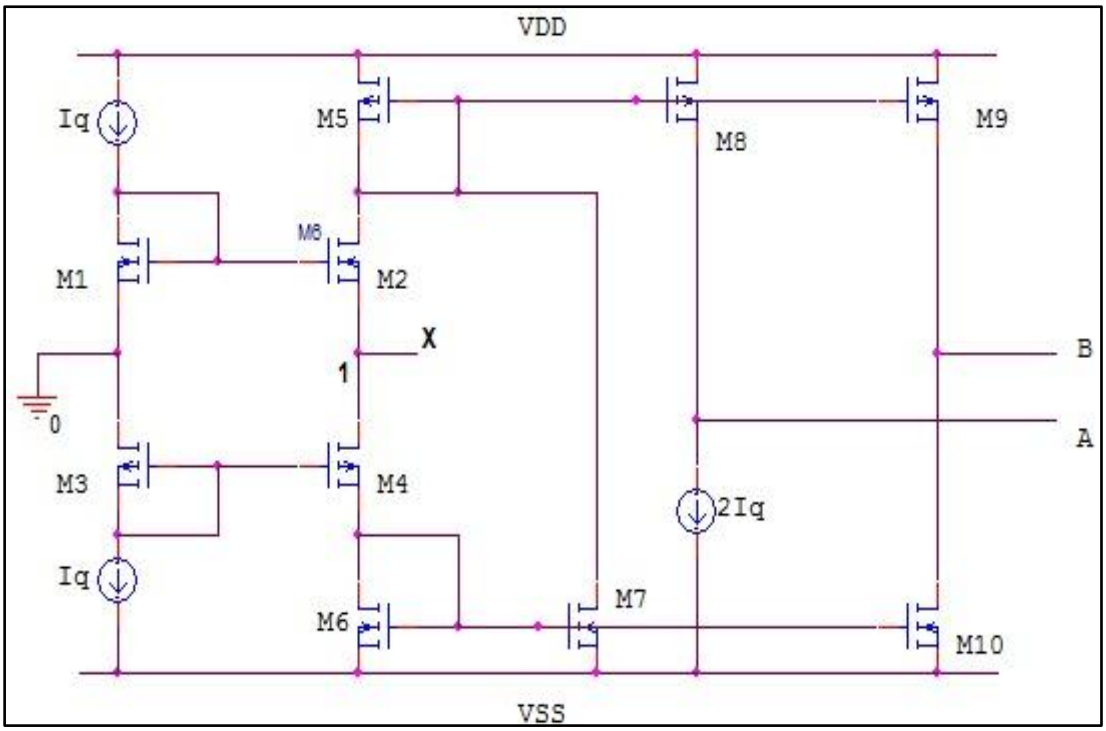

Fig 2.2 Linear And Square Block

2.3.2 ANALYSIS OF LINEAR AND SQUARE GENERATOR

Transistors M1-M4 form a translinear loop such that sum of voltages in clockwise direction equals the sum of voltages in anti-clockwise direction around the loop. It is assumed that transistors M1-M2 and M3-M4 are matched and all operate in saturation region. The equation leading to squarer and linear term as derived as follows:

$$V_{GS1} + V_{SG3} = V_{GS2} + V_{SG4} \tag{2.5}$$

$$\sqrt{\frac{I_{D1}}{\mu_n (W/L)_1}} + \sqrt{\frac{I_{D3}}{\mu_p (W/L)_3}} = \sqrt{\frac{I_{D2}}{\mu_n (W/L)_2}} + \sqrt{\frac{I_{D4}}{\mu_p (W/L)_4}} \tag{2.6}$$

But since transistors are matched and their transconductance are equal i.e. $\beta_n = \beta_p$. Hence,

$$2\sqrt{I_{D1}} = \sqrt{I_{D2}} + \sqrt{I_{D4}} \quad (2.7)$$

But, $I_{D1} = I_q$, thus we have

$$2\sqrt{I_q} = \sqrt{I_{D2}} + \sqrt{I_{D4}} \quad (2.8)$$

Now at node 1, we have

$$I_{D2} + x = I_{D4} \quad (2.9)$$

After solving equation (2.8) and (2.9) we get,

$$I_{D2} = I_q - \frac{x}{2} + \frac{x^2}{16I_q} \quad (2.10)$$

$$I_{D4} = I_q + \frac{x}{2} + \frac{x^2}{16I_q} \quad (2.11)$$

Adding equation (2.10) and (2.11) results gives,

$$I_{D2} + I_{D4} = 2I_q + \frac{x^2}{8I_q} \quad (2.12)$$

From figure 2.2 we have,

$$I_{D5} = I_{D2} + I_{D4} \quad (2.13)$$

Now current I_{D5} is copied with the help of M8 transistor and $2I_q$ is subtracted from this current value such that at node A we get,

$$I_A = \frac{x^2}{8I_q} \quad (2.14)$$

Now scaling of current I_{D5} is done by the factor of 2 which gives,

$$\frac{I_{D5}}{2} = I_q + \frac{x^2}{16I_q} \tag{2.15}$$

Copying this current through transistor M9 and subtracting I_{D4} from equation (2.15) with the help of copier transistor M10 gives,

$$\frac{I_{D5}}{2} - I_{D4} = -\frac{x}{2} \tag{2.16}$$

Which is done at node B, giving current I_B as,

$$I_B = -\frac{x}{2} \tag{2.17}$$

Equation (2.14) and equation (2.17) i.e. I_A and I_B can be used to approximated functions up to second order.

The above circuit has been simulated by the author [5] in 0.8um CMOS technology. But the drawbacks of the above circuit are mismatch in transconductances of transistors when short channel length is considered which is analyzed below. Also matching of transistor's aspect ratio is also tedious task.

2.3.3 DEVIATION FROM IDEAL CHARACTERSTICS

Since in above block it has been assumed that the transistors hold exact square law equation and transconductances are equal. But as we come to small channel length transistors our assumptions deviates from ideal condition due to second order effects that plays their role which are channel-length modulation, velocity saturation, body effect and decrement in mobility. These above parameters results in transconductance mismatch and contribute in error [5].

2.3.4 SIMULATION

The above circuit is simulated for large channel condition and deviation from ideal behavior for its short channel length is observed and its less maximum operation range have been shown in the simulation below in Fig 2.3, Fig 2.4, Fig 2.5 and Fig 2.6 using 0.35um CMOS technology in PSPICE A/D. Keeping in mind that at room temperature electron mobility is approximately twice that of hole mobility in

extrinsic semiconductor, transistor's aspect ratio has been chosen accordingly. The biasing currents I_q have been made equal to 0.125uA in order to make scaled square term equal to simple square term. The circuit is tested at power supply of ±1V.

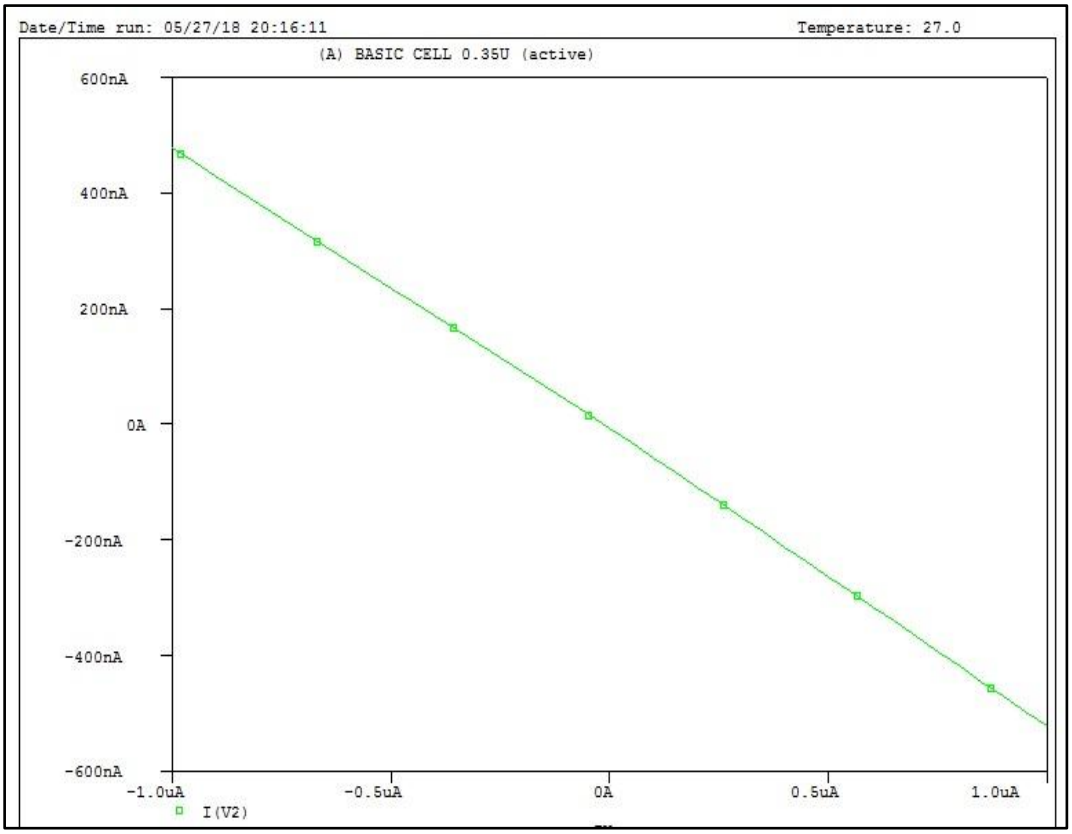

Fig 2.3 Output of linear term for long channel length

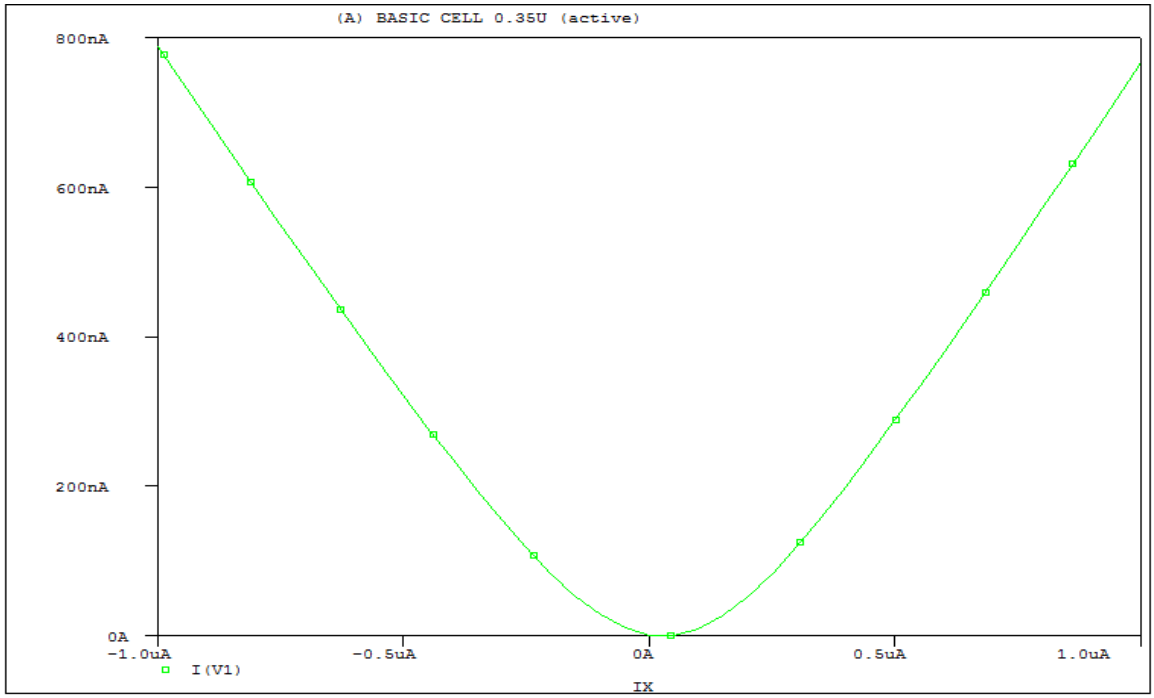

Fig 2.4 Square results for long channel length

One of the drawbacks of this circuit can be observed from Fig 2.4 that there is loss of signal i.e. as we move towards ±1uA there is lose in its output. Also this circuit is tested for its maximum operating range then it results in great loss of signal for exceeding input current more than ±2uA. Following graphs will present the output for short channel lengths, and deviations will be observed significantly.

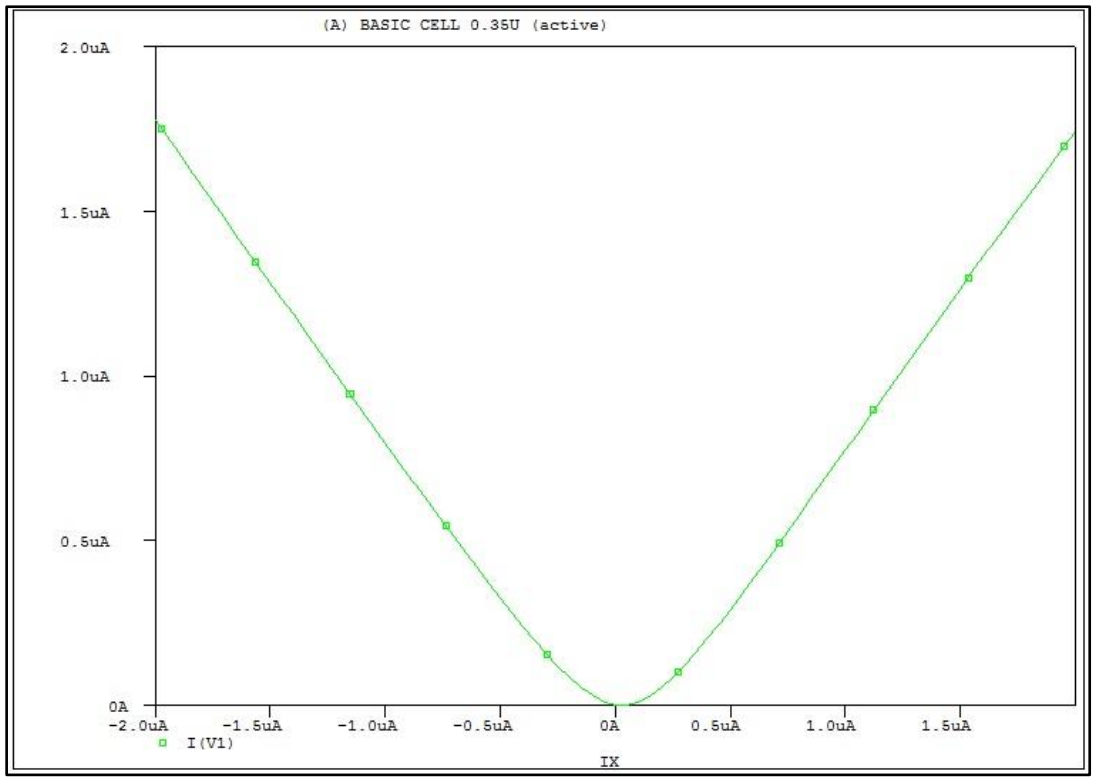

Fig 2.5 Square result for Short channel length

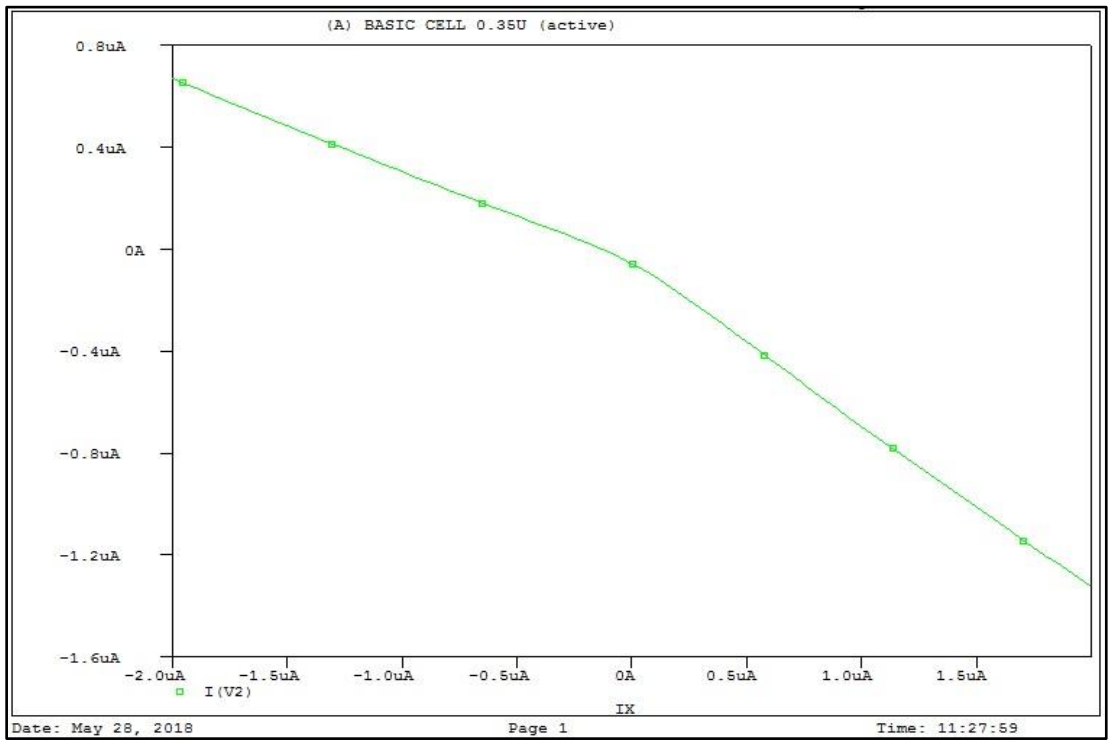

Fig 2.6 Linear result for short channel length

Now it can be easily observed from Fig 2.5 and Fig 2.6 that as we implement short channel length transistors matching of transistors comes into role because of short channel length parameters like channel length modulation etc. and it can be observed in Fig 2.5 that there is significant loss of signal as we increase its input range.

This is the major reason why in this dissertation bipolar circuits are implemented in latter chapter. But before we move to work implemented there are few more circuits that have been reviewed and used for implementation of functions that are implemented.

2.3.5 STANDARD SQUARER CIRCUIT

The analysis of this block presented in [6] is performed below for literature review purpose and for comparison purpose with the presented block in chapter 3.

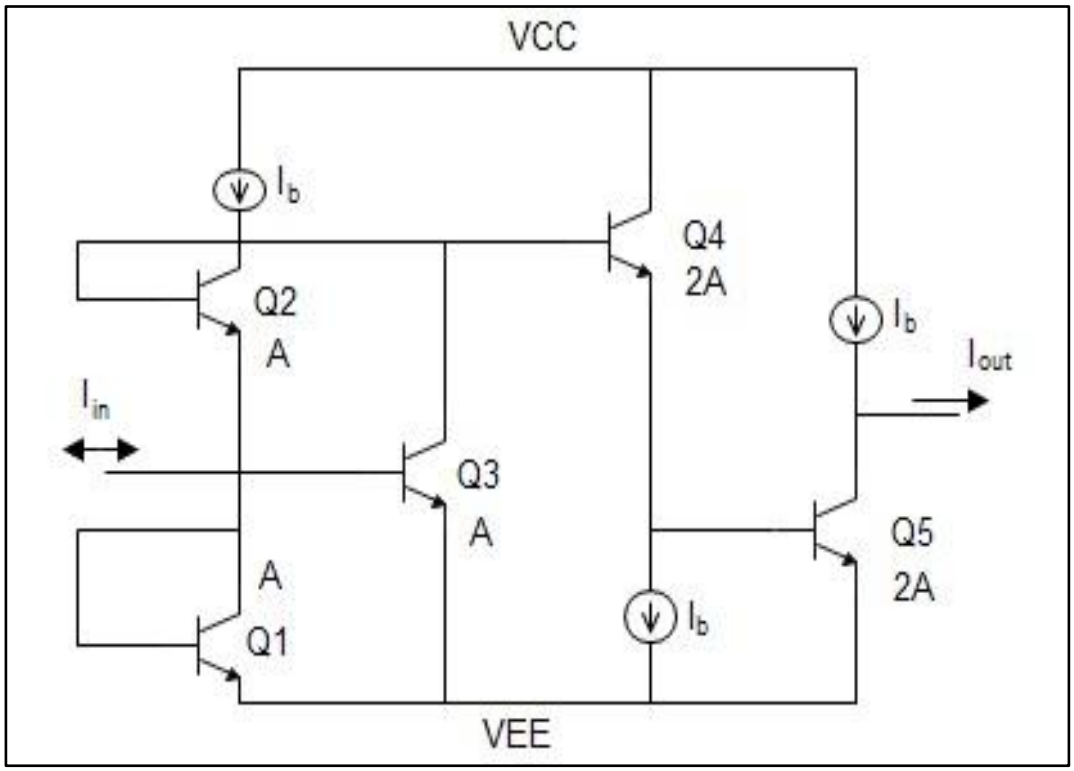

Fig 2.7 Standard Square Circuit

It should be noted here that Q4 and Q5 have double the area of Q1-Q3.

Considering the translinear loop containing Q1, Q2, Q4 and Q5, we have

$$I_{C1}I_{C2} = \frac{I_{C4}}{2}\frac{I_{C5}}{2} \tag{2.18}$$

$$I_{C1} = I_{C2} \pm I_{in} = I_{C3} \tag{2.19}$$

And,

$$I_{C2} = I_b - I_{C3} \tag{2.20}$$

$$I_{C4} = I_b \tag{2.21}$$

$$I_{C5} = I_b - I_{out} \tag{2.22}$$

Adding equations we get,

$$I_{C2} = \frac{I_b \mp I_{in}}{2} \; and \; I_{C1} = \frac{I_b \pm I_{in}}{2}$$

Placing the value of I_{C2} and I_{C1}, also I_{C4} and I_{C5} in equations we get,

$$I_{out} = \frac{I_{in}^2}{I_b} \tag{2.23}$$

The above equation is derived by neglecting the effect of common-emitter gain and base current equal to zero.

The PSPICE simulation results for this circuit is shown in Fig 2.8 below where we have used transistors NR200N and PR200N of ALA400 transistor array of AT&T company. Keeping the value of bias current I_b = 1uA and input current range to ±1.5uA.

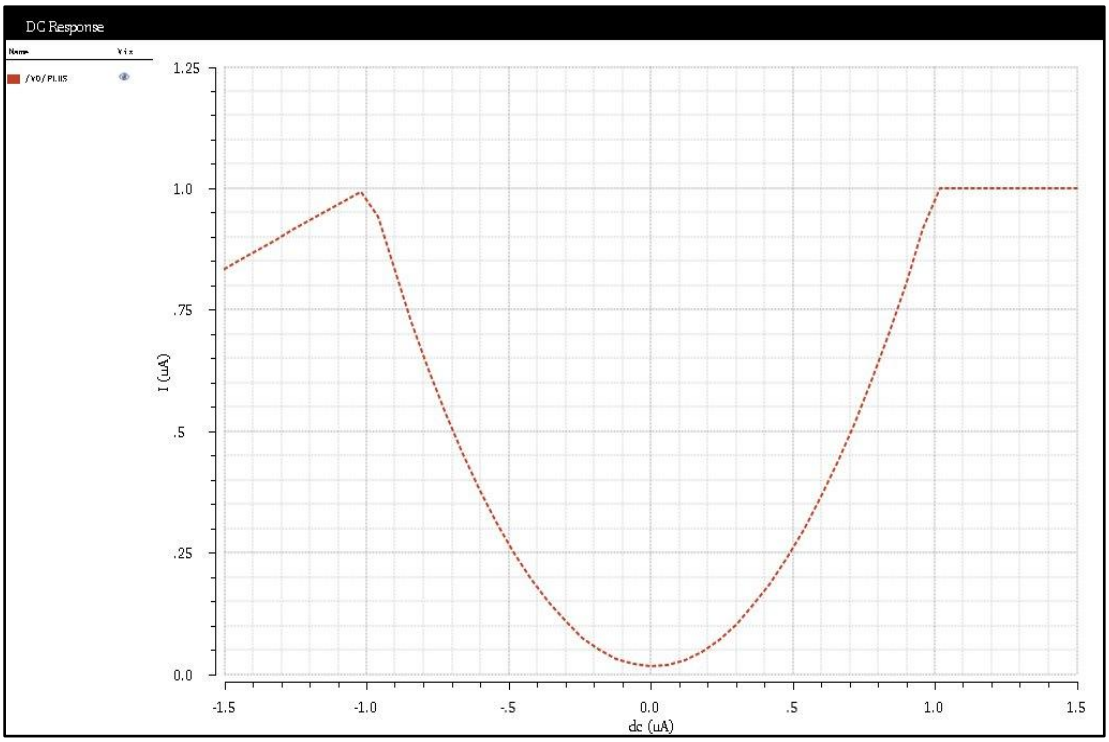

Fig 2.8 DC characteristics of Standard square block

It can be easily observed that the circuit output saturates at 1uA in both the quadrants. This drawback of maximum operating range is over came in proposed circuit in chapter 3.

2.4 LOG AND EXPONENTIAL BLOCKS

Several logarithmic and exponential blocks have been presented in [7] [8] [9]. Out of which logarithmic and exponential blocks are presented in [7] with bipolar implementation is discussed below.

2.4.1 LOGARITHMIC BLOCK

It consists of four bipolar transistors Q1-Q4, as shown in Fig 2.9, where input to this circuit is current and output is taken to be in voltage [7]. Derivation of input-output relationship and simulation part is shown in following part.

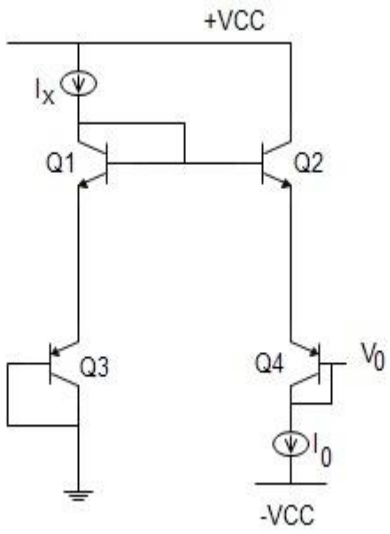

Fig 2.9 Logarithimic Block

2.4.2 ANALYSIS OF LOGARITHMIC BLOCK

Since emitter of transistors Q1 and Q3 are at same potential and similarly emitter of transistors Q2 and Q4 are also at same potential thus $V_{E1} = V_{E3}$ and $V_{E2} = V_{E4}$. Keeping this in mind we start with the derivation as follows:

$$I_X = I_S exp\left(\frac{V_{BE1}}{V_T}\right) \tag{2.24}$$

Also,

$$I_X = I_S exp\left(\frac{V_{EB3}}{V_T}\right) \tag{2.25}$$

But $V_{B3} = 0$, hence

$$V_{E3} = V_T \ln\left(\frac{I_X}{I_S}\right) = V_{E1} \tag{2.26}$$

Therefore,

$$V_{B1} = 2V_T \ln\left(\frac{I_X}{I_S}\right) = V_{B2} \quad (2.27)$$

Now $V_{B4} = V_0$, thus

$$V_{E4} = V_T \ln\left(\frac{I_0}{I_S}\right) + V_0 = V_{E2} \quad (2.28)$$

And

$$V_{B2} - V_{E2} = V_T \ln\left(\frac{I_0}{I_S}\right) \quad (2.29)$$

From equations we get:

$$V_0 = 2V_T \ln\left(\frac{I_X}{I_0}\right) \quad (2.30)$$

Equation (2.30) gives the relationship between voltage and current in logarithmic form. Its simulation is done in PSPICE A/D with I_0 = 1mA and using bipolar transistors NR200N and PR200N of ALA400 transistor array of AT&T company. Fig 2.10 below shows the DC transfer characteristics.

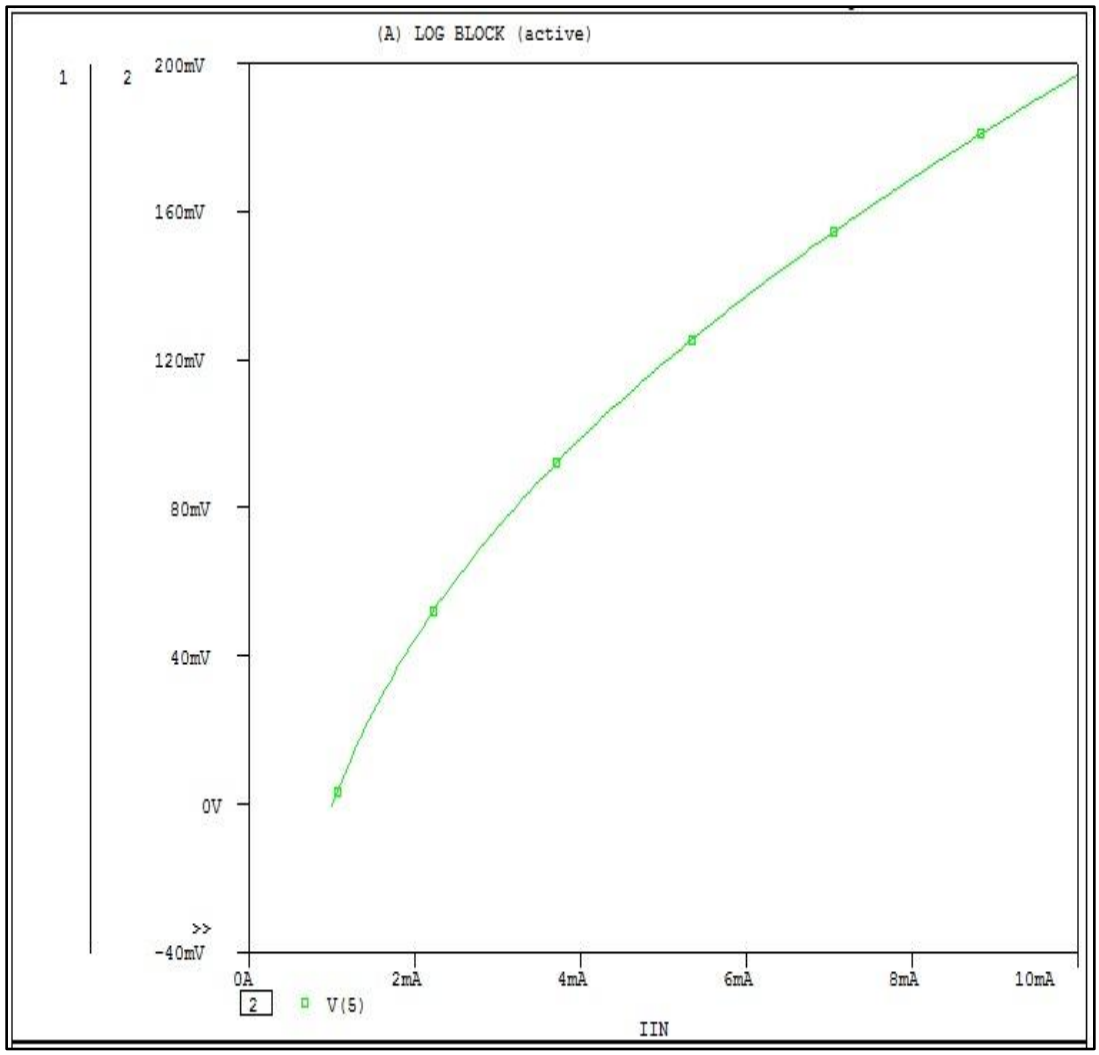

Fig 2.10 Logarithmic simulated result

2.4.3 EXPONENTIAL BLOCK

It consists of four transistors Q1-Q4 as shown in Fig 2.11 such that the relationship between input and output parameters i.e. differential voltage and current respectively is exponential. The input signal can be made single ended voltage by making one of the voltages to ground and the other to voltage signal [7]. The relationship and simulation part of the exponential block in shown below.

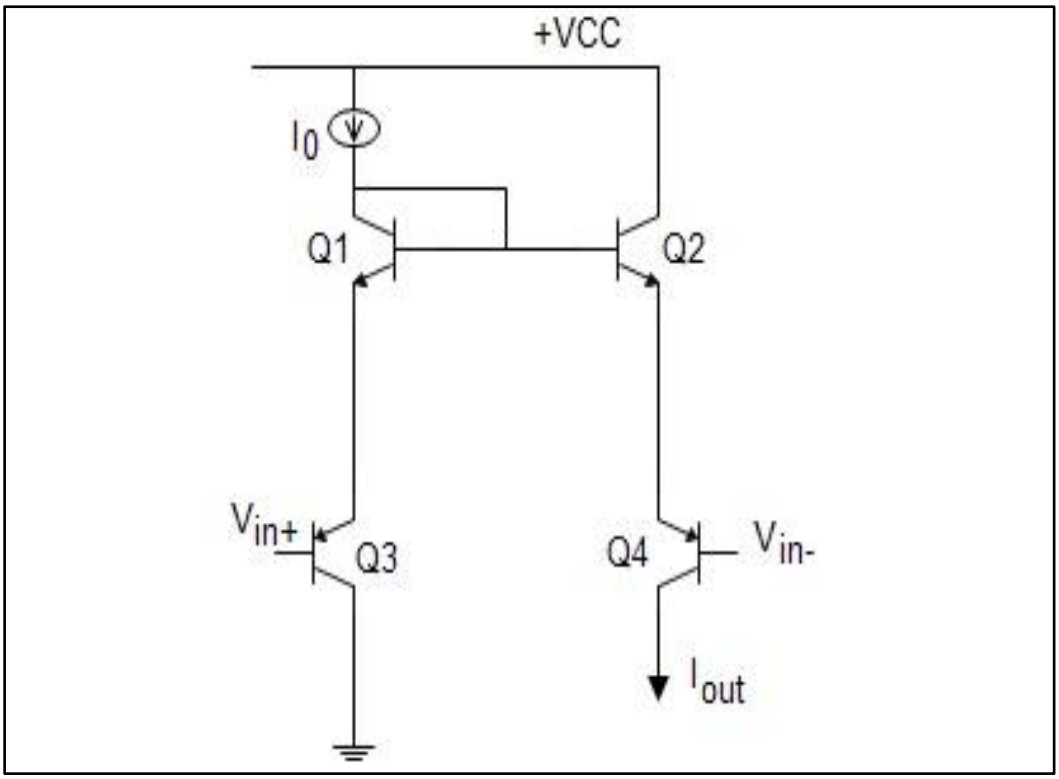

Fig 2.11 Exonential Circuit

2.4.4 ANALYSIS OF EXPONENTIAL BLOCK

Before moving to derivation part it is very important to keep it in mind from Fig 2.11 that emitter voltages of transistors Q1 and Q3 are equal as well as emitter voltages of transistors Q2 and Q4 are also equal.

From the fig 2.11 we have,

$$I_0 = I_S exp\left(\frac{V_{BE1}}{V_T}\right) \tag{2.31}$$

$$V_{B1} = V_T \ln\left(\frac{I_0}{I_S}\right) + V_{E1} \tag{2.32}$$

Or,

$$V_{B1} = V_T \ln\left(\frac{I_0}{I_S}\right) + V_{in+} + V_T \ln\left(\frac{I_0}{I_S}\right) \tag{2.33}$$

Since, $V_{E1} = V_{E3}$

Therefore,

$$V_{B1} = 2V_T \ln\left(\frac{I_0}{I_S}\right) + V_{in+} \quad (2.34)$$

Similarly,

$$V_{E4} = V_T \ln\left(\frac{I_{0ut}}{I_S}\right) + V_{in-} \quad (2.35)$$

And,

$$V_{B2} - V_{E2} = V_T \ln\left(\frac{I_{out}}{I_S}\right) \quad (2.36)$$

But $V_{B2} = V_{B1}$ and $V_{E2} = V_{E4}$, keeping the value of V_{B1} in place of V_{B2} in equation (2.36) from equation (2.34) and also the value of V_{E4} in place of V_{E2} in equation (2.36) from equation (2.35) we get relationship as follows:

$$I_{out} = I_0 exp\left(\frac{V_{in+} - V_{in-}}{2V_T}\right) \quad (2.37)$$

The simulation of the above circuit is performed in PSPICE A/D, using transistors NR200N and PR200N parameters of ALA400 transistor array from AT&T company, with VCC at 1.7V, I_0 = 1mA, and varying the positive input voltage from 0mV to 100mV, and keeping negative terminal voltage to ground potential. The DC characteristic of the circuit is shown in Fig 2.12 below:

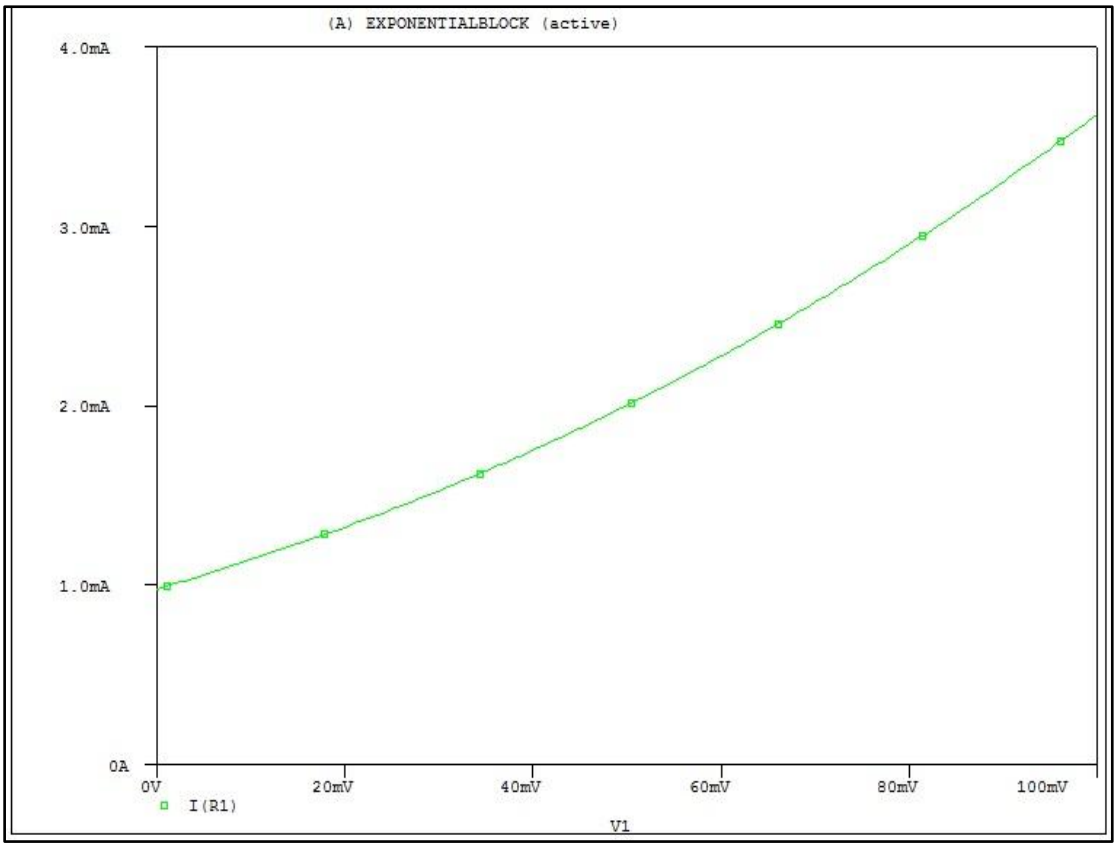

Fig 2.12 DC characteristics of exponential block

2.5 TRANSLINEAR PRINCIPLE BASED CURRENT MODE SQUARE ROOTING BLOCK

The circuit used for finding out square root of the given value is based on translinear principle [1], this circuit [10] consists of bipolar transistors as shown in Fig 2.13 below. This circuit is made up of translinear loop from Q1-Q4. Current mirrors are used to generate the square root of current with symmetry about x-axis. This block will be used latter in realization of elliptic curve which is one of the major applications of this dissertation which is an important technique for security in Cryptography.

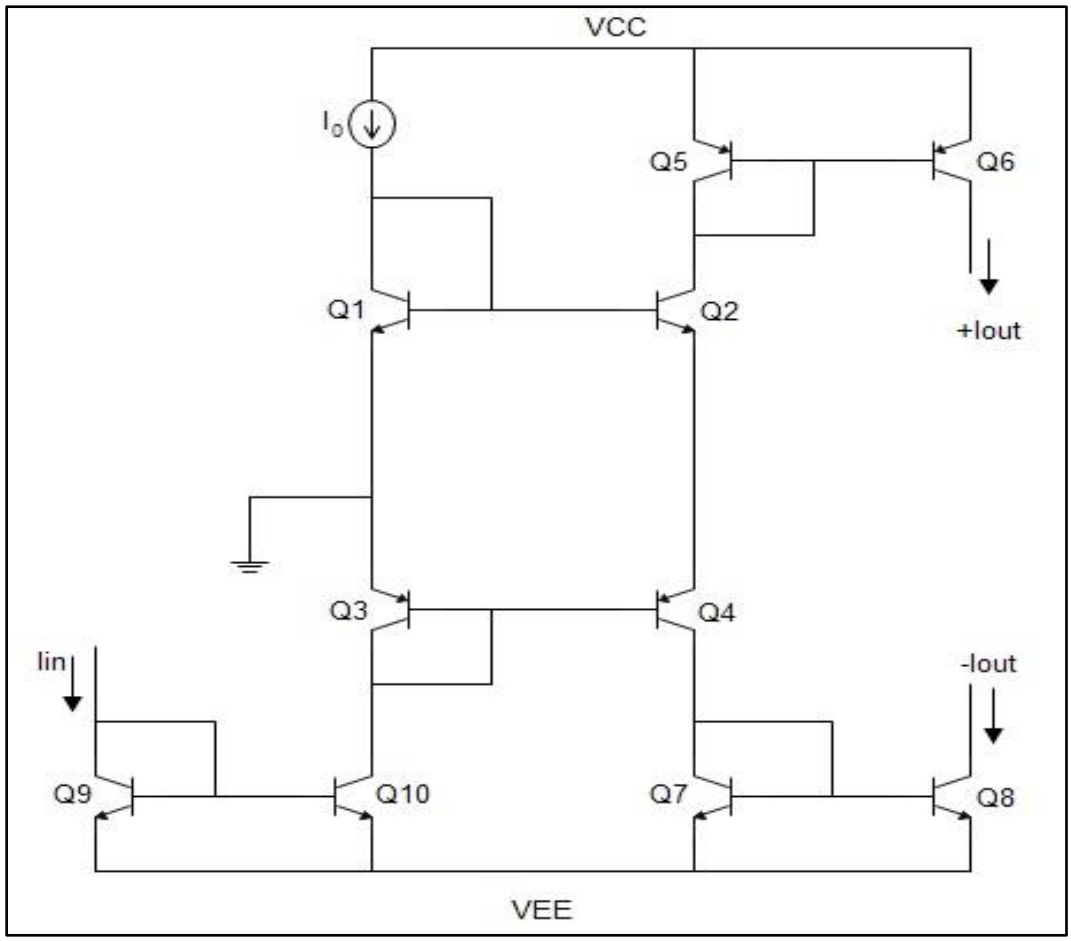

Fig 2.13 Translinear Based square root circuit

2.5.1 DERIVATION AND SIMULATION OF TRANSLINEAR BASED SQUARE ROOT BLOCK

From translinear loop Q1-Q4, we have

$$V_{BE1} + V_{EB3} = V_{BE2} + V_{EB4} \tag{2.38}$$

Therefore,

$$V_T \ln\left(\frac{I_0}{I_S}\right) + V_T \ln\left(\frac{I_{in}}{I_S}\right) = V_T \ln\left(\frac{I_{out}}{I_S}\right) + V_T \ln\left(\frac{I_{out}}{I_S}\right) \tag{2.39}$$

Thus,

$$I_0 I_{in} = (I_{out})^2 \tag{2.40}$$

Hence,

$$I_{out} = \pm\sqrt[2]{I_{in} I_0} \tag{2.41}$$

Equation (2.41) gives us the output current as square root of product of input current and biasing current in both 1st and 4th quadrant.

Keeping all transistor's emitter width equal and keeping I_0 = 1uA along with VCC = +3.65V and VEE = - 3.65V, the simulation is performed in PSPICE A/D using NR200N and PR200N model of ALA400 transistor array from AT&T company. The simulation is shown below in Fig 2.14.

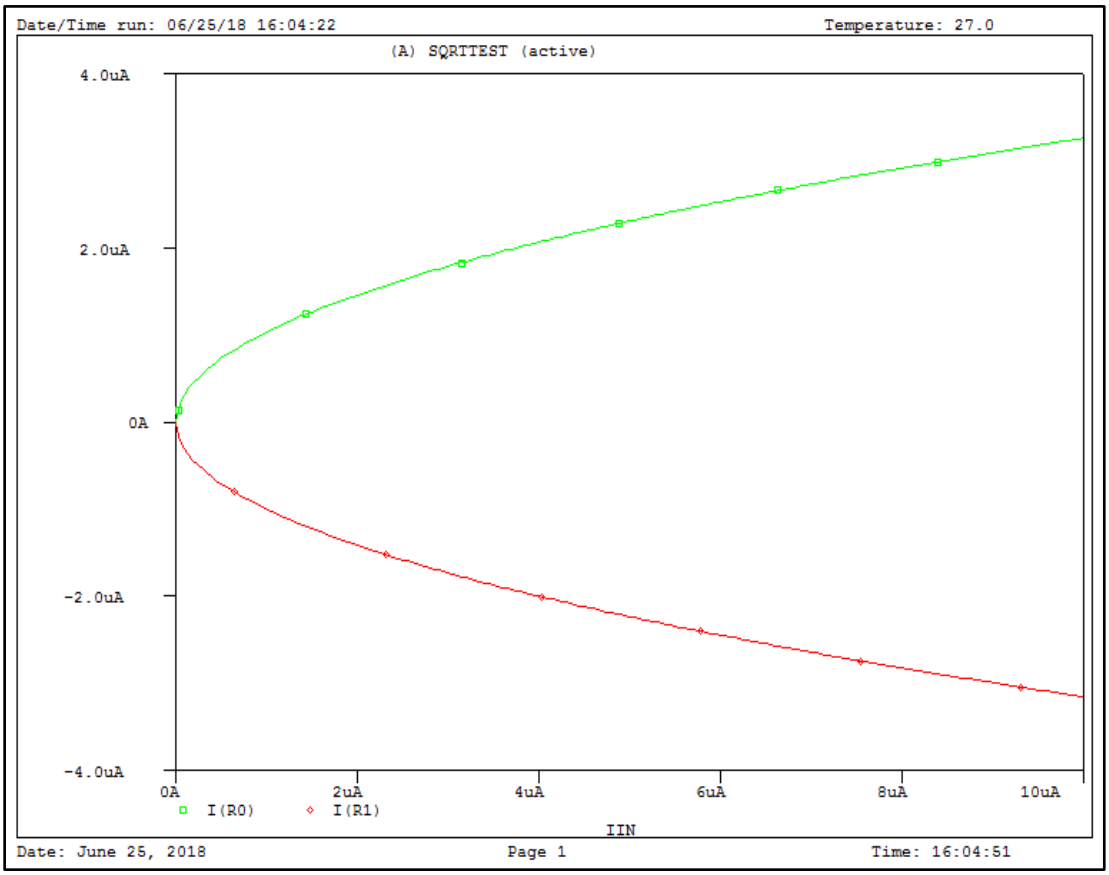

Fig 2.14 DC characteristics of Square root circuit

It can be observed that the circuit has large operating range as the input current is varied from 0uA to 10uA and we have received significant output for its square root shown in Fig 2.14.

2.6 SQUARE ROOT BLOCK USING CMOS

The circuit shown below consists on NMOS and PMOS transistors which is not based on translinear loop principle [1], circuit is mainly the application of current mirror, in this circuit the relationship between input and output is between voltage and current, where as current is the input and voltage as output. The circuit [11] is shown in Fig 2.15 and its simulation is shown in Fig 2.16 below.

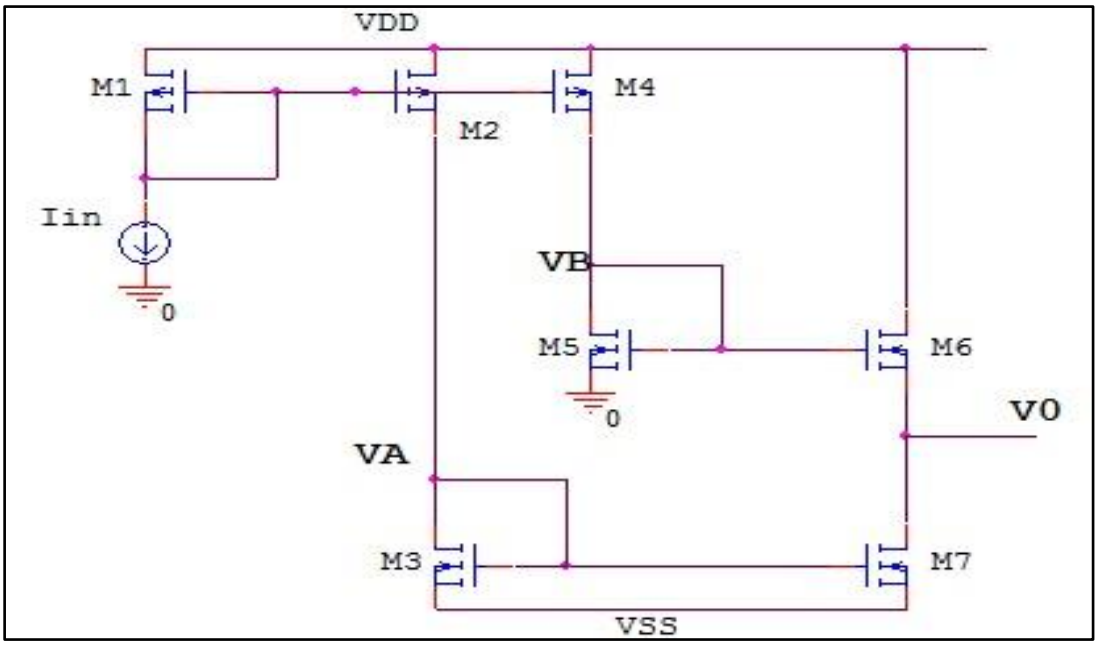

Fig 2.15 CMOS Square root circuit

Derivation of relationship between input and output and simulation results is shown below in following section.

2.6.1 IMPLEMENTATION OF SQUARE ROOT BLOCK

It can be observed from Fig 2.15 that transistors M1, M2 and M4 form a current mirror circuit, thus the same current I_{in} flows through transistor M4, and eventually through transistor M2, and M2 is connected to transistor M3 leading to same flow of current I_{in}, now transistors M3 and M7 also forms a current mirror

circuit, thus the M7 also flows current I_{in}. To be noted here is that transistor M5 aspect ratio is kept is scaled by the factor of 4 than other transistors in order to get square root relationship at node V_0.

It should be kept in mind that all the transistors operate in saturation region to follow the square law characteristic.

We have,

$$V_A = V_T + V_{SS} + \sqrt{\frac{I_{in}}{K_3}} \tag{2.42}$$

And

Where $K_1 = K_2 = \ldots\ldots = K_7 = K = \mu C_{ox}(W/L)/2$ (2.43)

$$\frac{1}{4}\left(\frac{W}{L}\right)_5 = \left(\frac{W}{L}\right)_6 \tag{2.44}$$

$$V_B = V_T + \sqrt{\frac{4I_{in}}{K_5}} \tag{2.45}$$

$$I_{D6} = K_6(V_B - V_0 - V_T)^2 \tag{2.46}$$

$$I_{D7} = K_7(V_A - V_{SS} - V_T)^2 \tag{2.47}$$

And $I_{D6} = I_{D7}$ (2.48)

Equating equations (2.46) and (2.47) and putting values from equation (2.42) and (2.45), we get

$$V_0 = \sqrt{\frac{I_{in}}{K}} \tag{2.49}$$

Equation (2.49) gives us the voltage as the square root of current with scaling factor K.

Simulation of this circuit is performed in PSPICE A/D using 0.35um CMOS technology keeping bias giving VDD = 1.75V and VSS = -1.75V, varying input range from 0uA to 12uA, a resistor of 1Kohm is connected at output node V_0 in order to observe the output. The characteristic observed is DC transfer characteristics shown in Fig 2.16, the aspect ratio and parameter model files for level 7 0.35um CMOS technology is presented in Appendix 1 and 2.

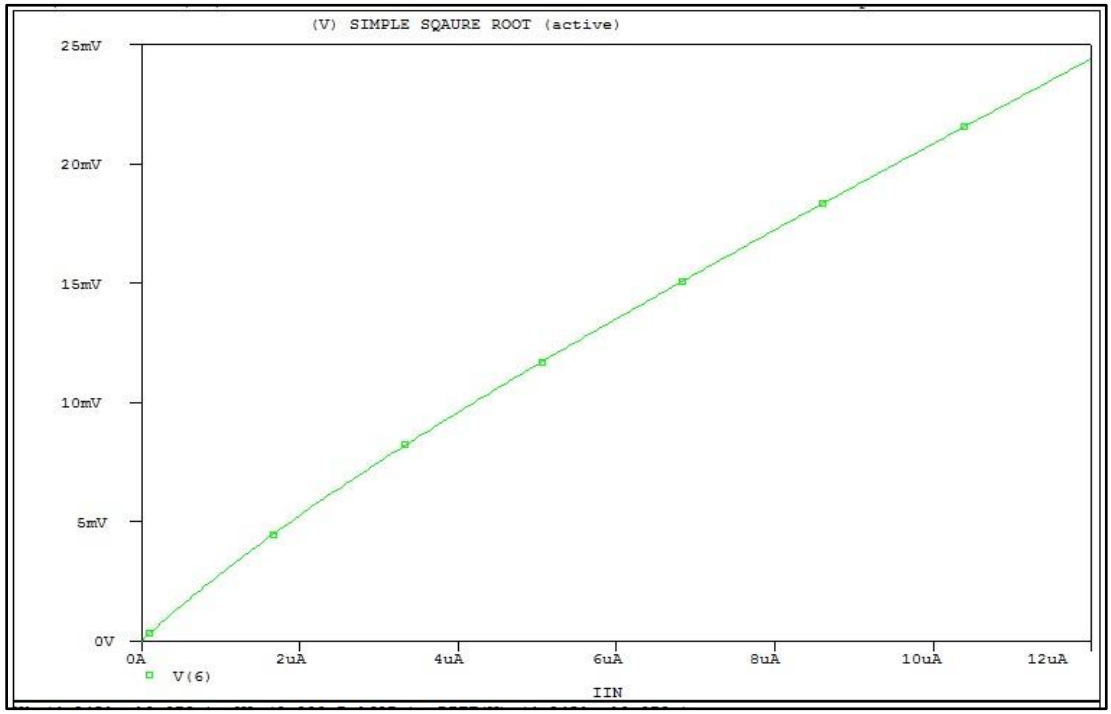

Fig 2.16 Simulated result for CMOS square root circuit

2.7 SIGMOIDAL FUNCTION

A Sigmoid Function [12] is a very useful non-linear signal processing element used extensively in artificial neural networks. These functions may be implemented using digital hardware which requires more power, more chip area as compared to analog implementation of the same [13]-[16]. An analog circuit implementation of the same has been presented in [12].

It is called resistive type because of its input-output characteristics which have current as input and voltage as output. There are other resistive type sigmoid function which were proposed earlier than this one [17] in which the transistors were

operating only off or saturation region due to sudden switching from off to saturation and vice-versa noise spikes was introduced. In this work [12] transistors are made operative in triode and saturation regions making it more smooth result and with very much precision.

Sigmoid function is generated using the following circuitry shown in Fig 2.17 consisting of six transistors M1-M6 where M5 and M6 are used to generate the gate voltage equal to half of the supply voltage i.e. VCC/2, there sizing is done accordingly. And rest four transistors are used to give sigmoid function.

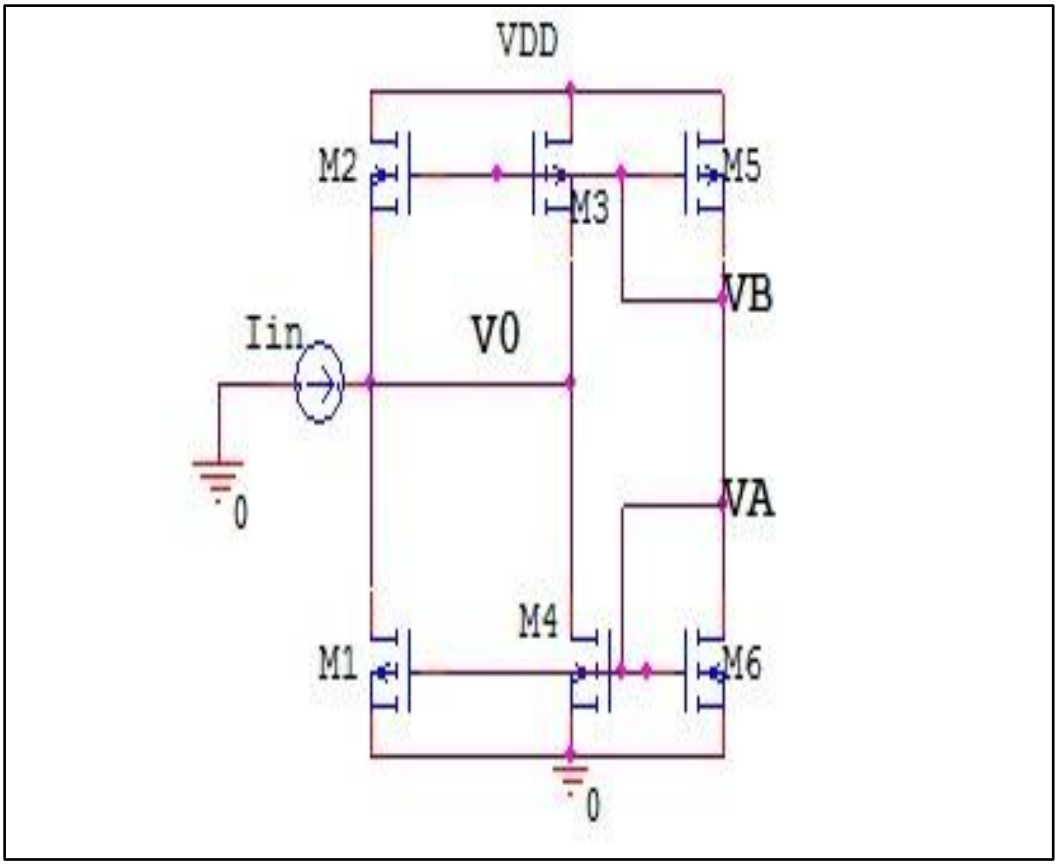

Fig 2.17 Sigmoid Function Generator

Table 2.1 Operating Region

Region	Iin	Vout	M1	M2	M3	M4
I	< 0	$0 \leq V_{out} \leq V_G - V_{in}$	off	sat	sat	Triode
II	< 0	$V_G - V_t \leq V_{out} \leq V_G$	off	off	sat	Sat
	= 0	$V_{out} = V_G$				
	>0	$V_G \leq V_{out} \leq V_G + \lvert V_t \rvert$				
III	>0	$V_G + \lvert V_t \rvert \leq V_{out} \leq Vdd$	sat	off	triode	Sat

In region I, the direction of current is outward causing very low voltage at output node. Thus making transistor M1 to turn off, M4 in triode and M2 and M3 is saturation region. Thus the relationship in this region is as follows:

$$I_{in} = -\frac{1}{2}k_n S_2 (V_G - V_{out} - V_t)^2 \left(1 + \lambda (V_{dd} - V_{out})\right) - \frac{1}{2}k_p S_3 (-V_G + V_{dd} - V_t)^2 \left(1 + \lambda (V_{dd} - V_{out})\right) + k_n S_4 \left((V_G - V_t)V_{out} - \frac{1}{2}V_{out}^2\right) \quad (2.50)$$

Where S is defined as (W/L)

Changes in operating region can be observed with the increase in input current, as M3-M4 switches to saturation region and other two are off entering into region II, which can be divided into three sub regions. First sub threshold region is when the current in negative, i.e. current coming out of M3 is more than the M4 sinking the current at output node. Now with the increase in output voltage, current through M3 decreases and through M4 increases resulting to voltage reaching at

$V_{dd}/2$, at this point no current flows in i.e. when input current is zero. In third sub region current becomes positive and the equation is followed as follows:

$$I_{in} = \frac{1}{2}k_n S_4(V_G - V_t)^2(1 + \lambda V_{out}) - \frac{1}{2}k_p S_3(V_{dd} - V_G - V_t)^2\big(1 + \lambda(V_{dd} - V_{out})\big) \quad (2.51)$$

The circuit enters into third region now where current is always positive. The output voltage corresponding to increase in current results in M1 to move into saturation and M3 to move into triode region but keeping rest of the two transistors in same regions as earlier. The equation in this region is as follows:

$$I_{in} = -k_p S_3\left((V_{dd} - V_G - V_t)(V_{dd} - V_{out}) - \frac{1}{2}(V_{dd} - V_{out})^2\right) + \frac{1}{2}k_p S_1(V_{out} - V_G - V_t)^2(1 + \lambda V_{out}) + \frac{1}{2}k_n S_4(V_G - V_t)^2(1 + \lambda V_{out}) \quad (2.52)$$

Note that for I_{in} equal to zero when $V_{out} = V_{dd}/2$, $k_pS_3 = k_nS_4$. And $S_2 = 2S_4$, $3S_1 = 4S_3$. This is done to keep the symmetry around $I_{in} = 0$.

The simulation is performed in PSPICE A/D using the 0.35um CMOS technology keeping the power supply VDD = 1.5V, and varying input current from -2uA to 2uA with the step size of 0.05uA, the aspect ratio and parameter model files for level 7 0.35um CMOS technology is presented in Appendix 1 and 2. The input – output characteristics of the implemented sigmoid function is shown in Fig 2.18 below. This circuit's improved version is shown in latter chapter 4, which is operated in current mode and is framed using Taylor series approximation.

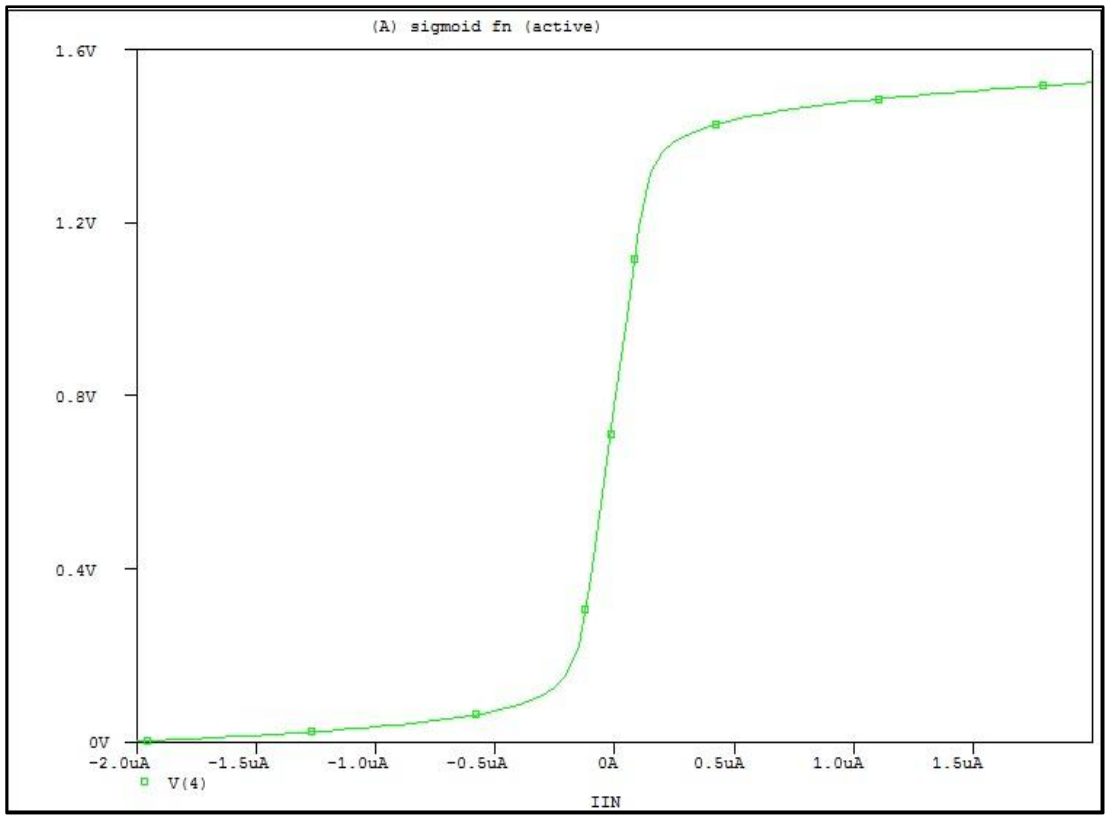

Fig 2.18 DC transfer characterstics of Sigmoid function

2.8 CONCLUSION

In this chapter we have presented various non linear blocks along with their simulation and operating range as an literature review, which have been already implemented. One of the blocks i.e. translinear based square rooting will be helpful in latter chapter as our major application of elliptic curve used in Cryptosystems.

REFERENCES

[1] B. Gilbert,"Translinear circuits: a proposed classification," *Electronics Letters*, vol.11,no.1,pp.14-16,1975.

[2] A. Naderi, A. Khoei, Kh. Haddi, H. Ghasemzadeh, "A New High Speed and Low Power Four-Quadrant CMOS Analog Multiplier in Current-Mode," *International Journal of Electronics and Communications (AEU)*, vol. 63, no. 9, pp. 769-775, 2009.

[3] H. Sajjadi-Kia, "An Analog Cell and Its Applications in Analog Signal Processing," *International Journal of the Circuit theory and Applications*, vol. 39, no.2,pp.195-201,2011.

[4] S. Minaei, E. Yuce, "New Squarer Circuits and a Current-Mode Full Wave Rectifier Topology Suitable for Integration," *Radioengineering*, vol. 19, no. 4, pp. 657-661,2010.

[5] M.T. Abuelma'atti, M.A. Alabsi, "A CMOS Analog Cell and its Applications in Analog Signal Processing," *International Journal Of Electronics*, vol. 93, No.4,2006,251-267.

[6] B. Gilbert, "A Precise Four-Quadrant Multiplier with Subnanosecond Response," *IEEE J. Solid – State Circuits*, vol. SC-3, 365-373,1968.

[7] R. Groza, L. Festila, E. Szopos, "Four Quadrant Log-Domain Analog Current Multiplier," *IEEE Int. Conf. on Automation, Quality and Testing, Robotics,* Cluj-Napoca,Romania,2008,pp.1-4244-2577-8/08.

[8] W. Liu, S.I. liu, "CMOS Exponential Function Generator," *Electronics Letters*, vol. 39, pp. 1-2,2003

[9] A. Motamed, C. Hwang, M. Ismail, "CMOS exponential Current-to-Voltage converter," *Electronics Letters*, vol. 33, pp. 998-1000,1997.

[10] M. Kumngern, K. Dejhan, "A New Translinear-Based Dual-Output Square-Rooting Circuit," *Active and Passive Electronic Components*,2008, Article ID623970.

[11] C. Sakul,"A CMOS Square Rooting Circuit," *International Technical Conference on Circuits/Systems, Computers and Communications*,2008,pp-537-540.

[12] G. Khodabandehloo, M. Mirhassani, M. Ahmadi, "Analog Implementation of a Novel Resistive-Type Sigmoidal Neuron," *IEEE trans. On VLSI sytems*, vol. 20,

No.4,2012.

[13] M.T. Tommiska, "Efficient digital implementation of the sigmoid function for reprogrammable logic," *IEE Proc. Comput. Digit. Techn.*, vol. 150, no. 6, pp. 403-411,2003.

[14] A.H. Namin, K. Leboeuf, R. Muscedere, H. Wu, M. Ahmadi, "Efficient hardware implementation of the hyperbolic tangent sigmoid function," *Proc. IEEE Int. Symp.CircuitsSyst.*,2009,pp.2117-2120.

[15] M. Mirhassani, M. Ahmadi, A. Jullien, "Robust low –sensitivity adaline neuron based on continuous valued number system," *J. Analog Integr. Circuit Signal Process.*, vol. 56, pp. 223-231, 2008.

[16] S.M. Gowda, B.J. Sheu, J. Choi, C.G. Hwang, J.S. Cable, "Design and characterization of analog VLSI neural network modules," *IEEE J. Solid –State Circuits*,vol.28,no.3,pp.301-313,1993.

[17] H. Djahanshahi, M. Ahmadi, G.A. Jullien, W.C. Miler, "Sensitivity study and improvements on a nonlinear resistive-type neuron circuit," *IEE Proc. – Circuits, DevicesSyst.*,vol.147,no.4,pp.237-242,2000.

CHAPTER 3

STANDARD MODULES FOR APPROXIMATION OF FUNCTIONS

3.1 INTRODUCTION

In the previous chapter we had presented a brief review of analog circuit realization of the non-linear building blocks along with basics of translinear circuit principle that will be helpful in further realization of blocks.

In current chapter we start with current mirrors and inverting current mirrors [1]. They have major application in developing the standard modules and approximated functions [2] discussed in this chapter and later in chapter 4. Realization of additional non linear building blocks has been done which have been used for functional approximation in later chapters. All blocks are realized in current mode which is advantageous as highlighted in earlier chapters. All the blocks are implementation of bipolar transistors hence provides the faster response. And have wide operating range. In this chapter we have also done exact analysis along with ideal analysis for the purpose of comparison. The DC transfer characteristics, transient analysis and AC analysis are done using PSPICE A/D simulation. The each block's comparison with ideal characteristic performed in MATLAB.

3.2 NON INVERTING CURRENT MIRROR AND INVERTING CURRENT MIRROR

Current mirrors are also known as current copier, which copies the input current at output transistor with some constant C, and whose value can be a positive integers or some fractional value except zero to maximum until the transistors remain in operating region. Non inverting current mirror have same direction of both input current and output current which are either in inward or outward direction, whereas inverting current mirror have opposite direction of input and output currents. The relation among input-output current and basic concept is discussed below.

3.2.1 NON INVERTING CURRENT MIRROR

It is also known as current copier which copies the input current in the same direction with some constant which is ratio of two transistor's area as shown in Fig 3.1 below.

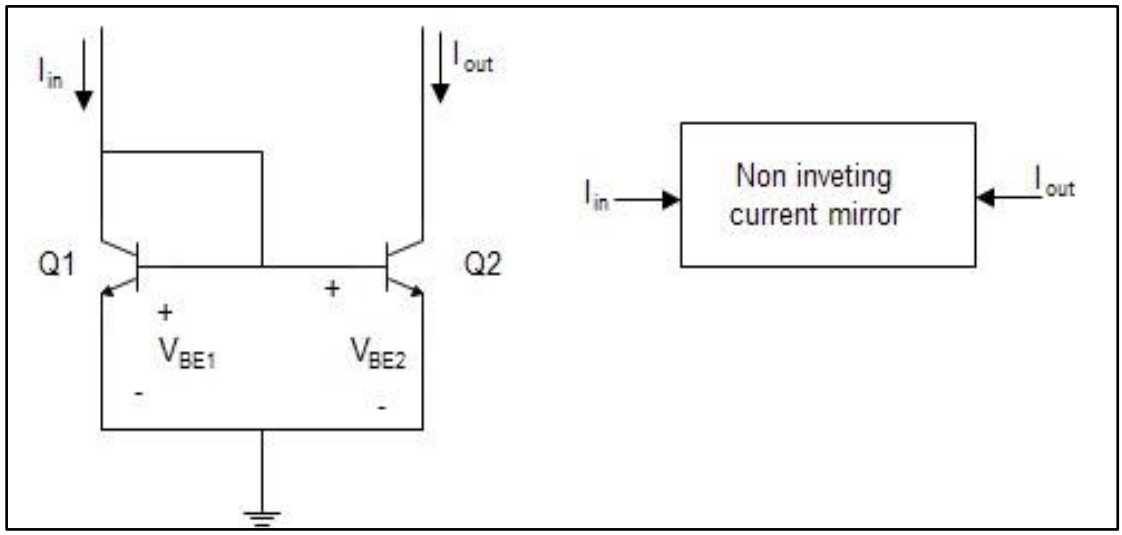

Fig 3.1 Non Inverting Current mirror

Base of two NPN transistors Q1 and Q2 are connected together and both transistor's emitter are at zero potential. Thus base-emitter voltage of both the transistors is equal.

$$V_{BE1} = V_{BE2} \tag{3.1}$$

And $V_{BEi} = V_T \ln\left(\frac{I_{Ci}}{I_{Si}}\right)$ where

I_{Ci} = Collector current of transistor

$I_{Si} \propto A_i$, reverse saturation current proportional to area or emitter width.

Thus

$$V_T \ln\left(\frac{I_{C1}}{I_{S1}}\right) = V_T \ln\left(\frac{I_{C2}}{I_{S2}}\right) \quad (3.2)$$

And $I_{C1} = I_{in}$, $I_{C2} = I_{out}$

$$I_{out} = \frac{A_2}{A_1} I_{in} \quad (3.3)$$

Or,

$$I_{out} = C I_{in} \quad (3.4)$$

Where C = area ratio of bipolar transistors

The value of C can be chosen by varying the emitter width of transistors. And it can be easily observed that the direction of output current is also inward as that of input hence named as non-inverting current mirror or current copier.

3.2.2 INVERTING CURRENT MIRROR

It is composed of four transistors, two NPN and other two PNP. Both similar transistors forming a current mirror pair, the basic objective of this Configuration is to invert the direction of input current. It also has a constant value C_K, which is ratio of product of transistors. The inverting configuration is shown in Fig 3.2 below.

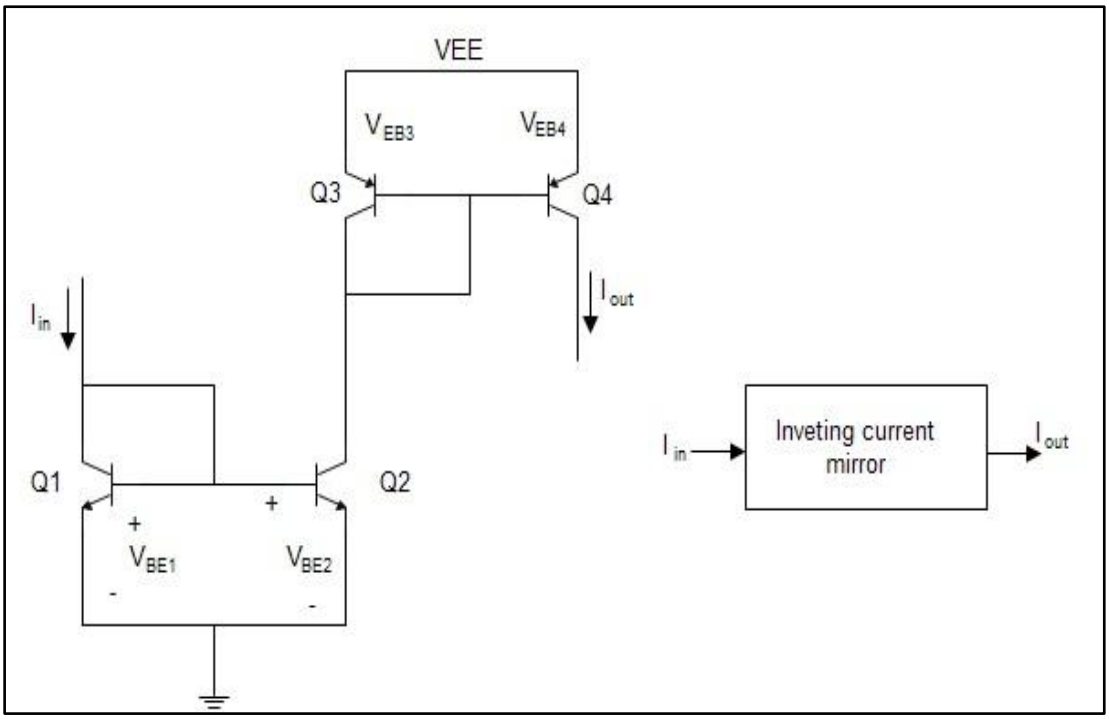

Fig 3.2 Inverting Current Mirror

From Fig 3.2 we have input-output current relation as follows:

$$I_{out} = \frac{A_2}{A_1}\frac{A_4}{A_3} I_{in} \tag{3.5}$$

Where $C_K = \frac{A_2}{A_1}\frac{A_4}{A_3}$

The value of C_K can modified accordingly with the variation in emitter width of four transistors defined as ratio of area of bipolar transistors.

3.3 LINEAR TERM GENERATOR/BLOCK

Inspired from current conveyors circuits as proposed in [3], that module can be used as one of the building block for generation of various functions. CCII has linear relation between input current and output current. The basic for the development of this circuit is translinear principle [4]. The circuit is shown in Fig 3.3 and the relation is derived in following part.

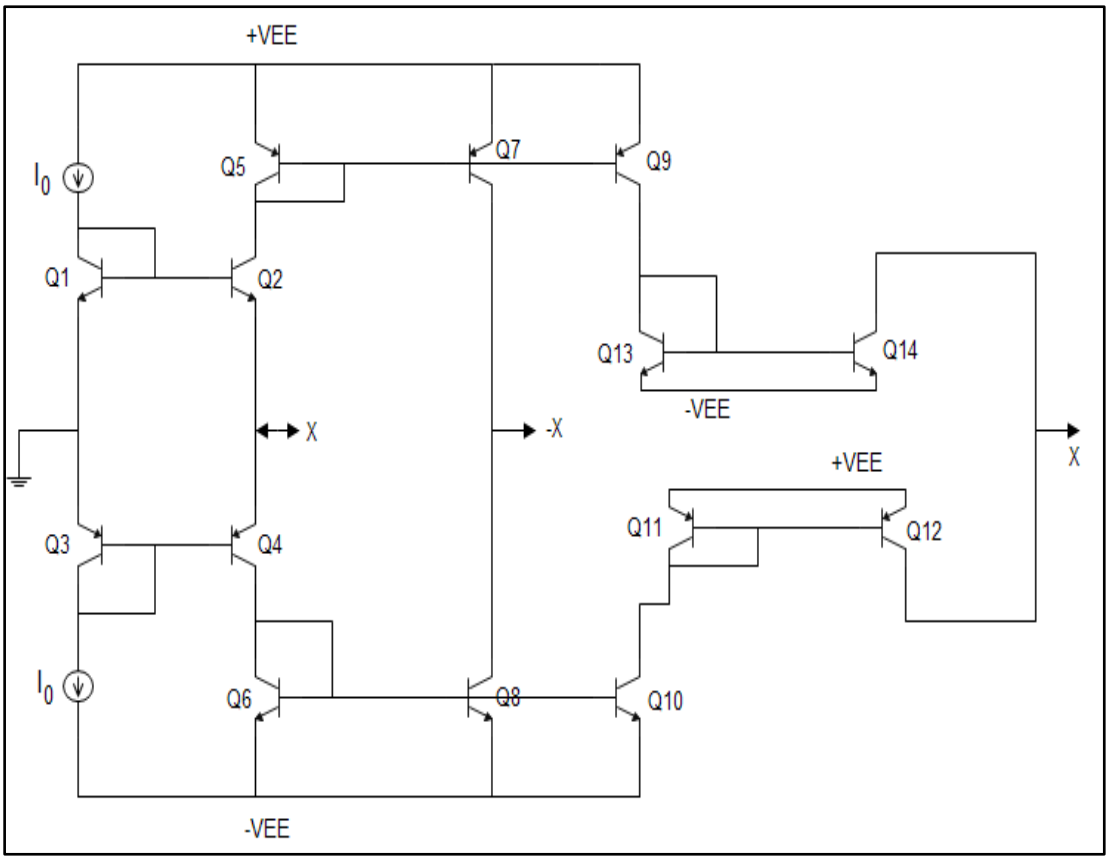

Fig 3.3 Linear Term Generator/block

3.3.1 IDEAL ANALYSIS OF LINEAR TERM GENERATOR

From the translinear loop shown above in Fig 3.3 we can write as,

$$V_{BE1} + V_{EB3} = V_{BE2} + V_{EB4} \tag{3.6}$$

Therefore,

$$I_0 I_0 = I_{C2} I_{C4} \tag{3.7}$$

And at input node,

$$I_{C4} = I_{C2} \pm X \tag{3.8}$$

From equation 3.7 and 3.8 we have,

$$I_{C2}^2 \pm X I_{C2} = I_0^2 \quad (3.9)$$

Or,

$$I_{C2} = \frac{\mp X \pm \sqrt{X^2 + 4I_0^2}}{2} \quad (3.10)$$

Now from equation 3.8 and 3.10 we have,

$$I_{C4} = \frac{\pm X \pm \sqrt{X^2 + 4I_0^2}}{2} \quad (3.11)$$

At output node we have,

$$I_{out\,1} = I_{C7} - I_{C8} \quad (3.12)$$

$$I_{out\,2} = I_{C12} - I_{C14} \quad (3.13)$$

From equation 3.14, 3.15, 3.16 and 3.17, we get result as,

$$I_{out\,1} = \mp X \text{ and } I_{out\,2} = \pm X \quad (3.14)$$

3.3.2 EXACT ANALYSIS OF LINEAR TERM GENERATOR

The effect of β (common-emitter current gain or collector to base current ratio) can be observed as the deviation from the ideal linear characteristics at higher values of input signal. Its effect is theoretically analyzed in the following part. With the help of translinear principle in above Fig 3.3 we have,

$$V_{BE1} + V_{EB3} = V_{BE2} + V_{EB4} \quad (3.15)$$

Therefore,

$$I_{C1}I_{C3} = I_{C2}I_{C4} \tag{3.16}$$

Also,

$$I_0 = I_{C1} + \frac{I_{C1}}{\beta_n} + \frac{I_{C2}}{\beta_n} \tag{3.17}$$

And,

$$I_0 = I_{C3} + \frac{I_{C3}}{\beta_p} + \frac{I_{C3}}{\beta_p} \tag{3.18}$$

Also,

$$I_{E4} = I_{E2} \pm X \tag{3.19}$$

That is,

$$I_{C4} + \frac{I_{C4}}{\beta_p} = I_{C2} + \frac{I_{C2}}{\beta_n} \pm X \tag{3.20}$$

After solving equations 3.16, 3.17, 3.18 and 3.20 we get I_{C2} and I_{C4} as follows in terms of β.

$$I_{C2} = \mp\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right]X \pm \frac{\beta_n\sqrt{X^2+4I_0^2}}{2(1+\beta_n)} \tag{3.21}$$

$$I_{C4} = \pm\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]X \pm \frac{\beta_p\sqrt{X^2+4I_0^2}}{2(1+\beta_p)} \tag{3.22}$$

From exact analysis of current mirrors formed by transistor pairs Q5-Q7-Q9 and Q6-Q8-Q10, gives us the collector current relation as,

$$I_{C7} = I_{C9} = \left(1 + \frac{2}{\beta_p}\right) I_{C5} = \left(1 + \frac{2}{\beta_p}\right) I_{C2} \tag{3.23}$$

$$I_{C8} = I_{C10} = \left(1 + \frac{2}{\beta_n}\right) I_{C6} = \left(1 + \frac{2}{\beta_n}\right) I_{C4} \tag{3.24}$$

And,

$$I_{out\,1} = I_{C7} - I_{C8} \tag{3.25}$$

$$I_{out\,2} = I_{C12} - I_{C14} \tag{3.26}$$

Solving for I_{out1} and I_{out2} we get,

$$I_{out\,1} = \mp\left(\left(1 + \frac{2}{\beta_p}\right)\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right] + \left(1 + \frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]\right) X \mp \left(\left(1 + \frac{2}{\beta_n}\right)\frac{\beta_p\sqrt{X^2 + 4I_0^2}}{2(1+\beta_p)} - \left(1 + \frac{2}{\beta_p}\right)\frac{\beta_n\sqrt{X^2 + 4I_0^2}}{2(1+\beta_n)}\right) \tag{3.27}$$

$$I_{out\,1} = \pm\left(1 + \frac{2}{\beta_p}\right)\left(1 + \frac{2}{\beta_n}\right)\left(\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right] + \frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]\right) X \pm \left(1 + \frac{2}{\beta_n}\right)\left(1 + \frac{2}{\beta_p}\right)\left(\frac{\beta_p\sqrt{X^2 + 4I_0^2}}{2(1+\beta_p)} - \frac{\beta_n\sqrt{X^2 + 4I_0^2}}{2(1+\beta_n)}\right) \tag{3.28}$$

Considering,

$$\sigma = \left(\left(1 + \frac{2}{\beta_p}\right)\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right] + \left(1 + \frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]\right)$$

$$\varphi = \left(\left(1+\frac{2}{\beta_p}\right)\left(1+\frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right] + \left(1+\frac{2}{\beta_p}\right)\left(1+\frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]\right)$$

And,

$$\delta(x) = \left(\left(1+\frac{2}{\beta_n}\right)\frac{\beta_p\sqrt{X^2+4I_0^2}}{2\left(1+\beta_p\right)} - \left(1+\frac{2}{\beta_p}\right)\frac{\beta_n\sqrt{X^2+4I_0^2}}{2(1+\beta_n)}\right)$$

$$\omega(x) = \left(1+\frac{2}{\beta_n}\right)\left(1+\frac{2}{\beta_p}\right)\left(\frac{\beta_p\sqrt{X^2+4I_0^2}}{2\left(1+\beta_p\right)} - \frac{\beta_n\sqrt{X^2+4I_0^2}}{2(1+\beta_n)}\right)$$

We can rewrite the equation 3.27 and 3.28 as,

$$I_{out\,1} = \mp\sigma X \mp \delta(x) \tag{3.29}$$

$$I_{out\,2} = \pm\varphi X \pm \omega(x) \tag{3.30}$$

As we know,

$$\left(1+\tfrac{2}{\beta_p}\right) \cong \left[\tfrac{1+\beta_n}{\beta_n}\right] \cong \left(1+\tfrac{2}{\beta_n}\right) \cong \left[\tfrac{1+\beta_p}{\beta_p}\right] \approx 1 \tag{3.31}$$

Hence $\delta(x) = \omega(x) \approx 0$, thus we have,

$$I_{out\,1} = \mp\sigma X \text{ and } I_{out\,2} = \pm\varphi X \tag{3.32}$$

Where σ ≈ 1, φ ≈ 1.

3.3.3 DC TRANSFER CHARACTERSTICS OF LINEAR TERM GENERATOR

The simulation is performed in PSPICE A/D using bipolar transistors NR200N and PR200N of ALA400 transistor array from AT&T company, the value of power supply is kept at ±3.65V, and I_0 = 1uA. This circuit is analyzed for operating range of ±10mA. The DC transfer characteristic is shown in Fig 3.4 as below.

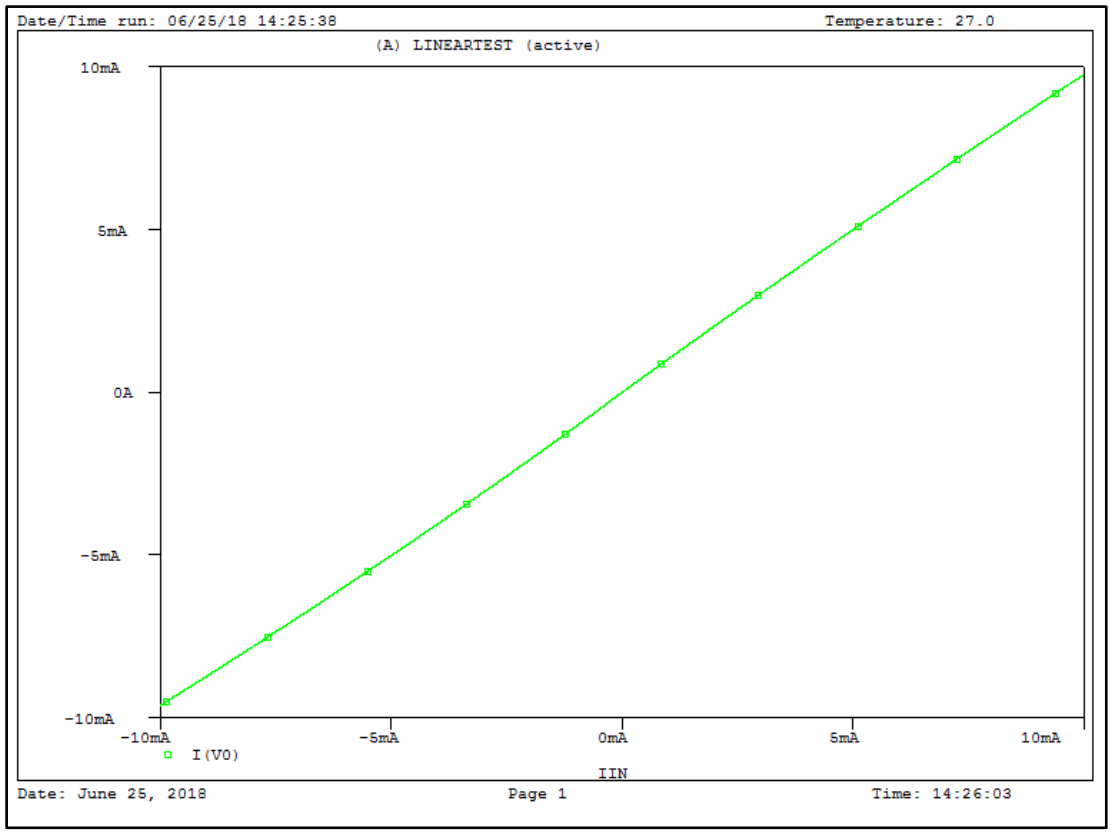

Fig 3.4 DC characterstics of Linear Term generator

3.3.4 TRANSIENT ANALYSIS OF LINEAR BLOCK

The transient analysis is performed in PSPICE A/D with power supply voltage equal to ±3.65 V. The NR200N and PR200N transistor models of ALA400 transistor array from AT&T company are used for simulation. Transient analysis is done for varying the time from 0ms to 2ms, and applying the input signal at

frequency 1KHz and amplitude 1uA. Fig 3.5 and Fig 3.6 below shows the analysis for both positive linear term and negative linear term.

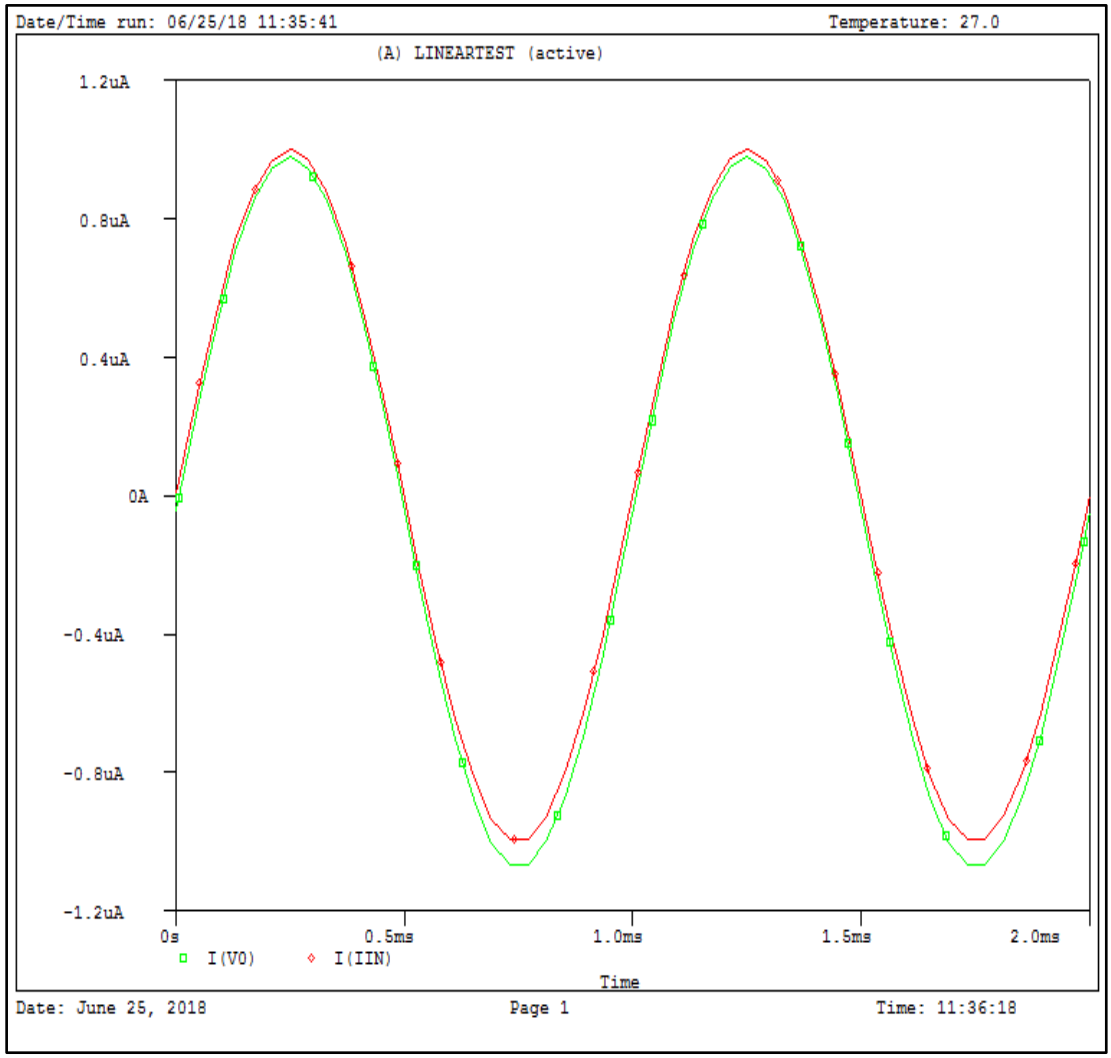

Fig 3.5 Transient response of positive linear term generator

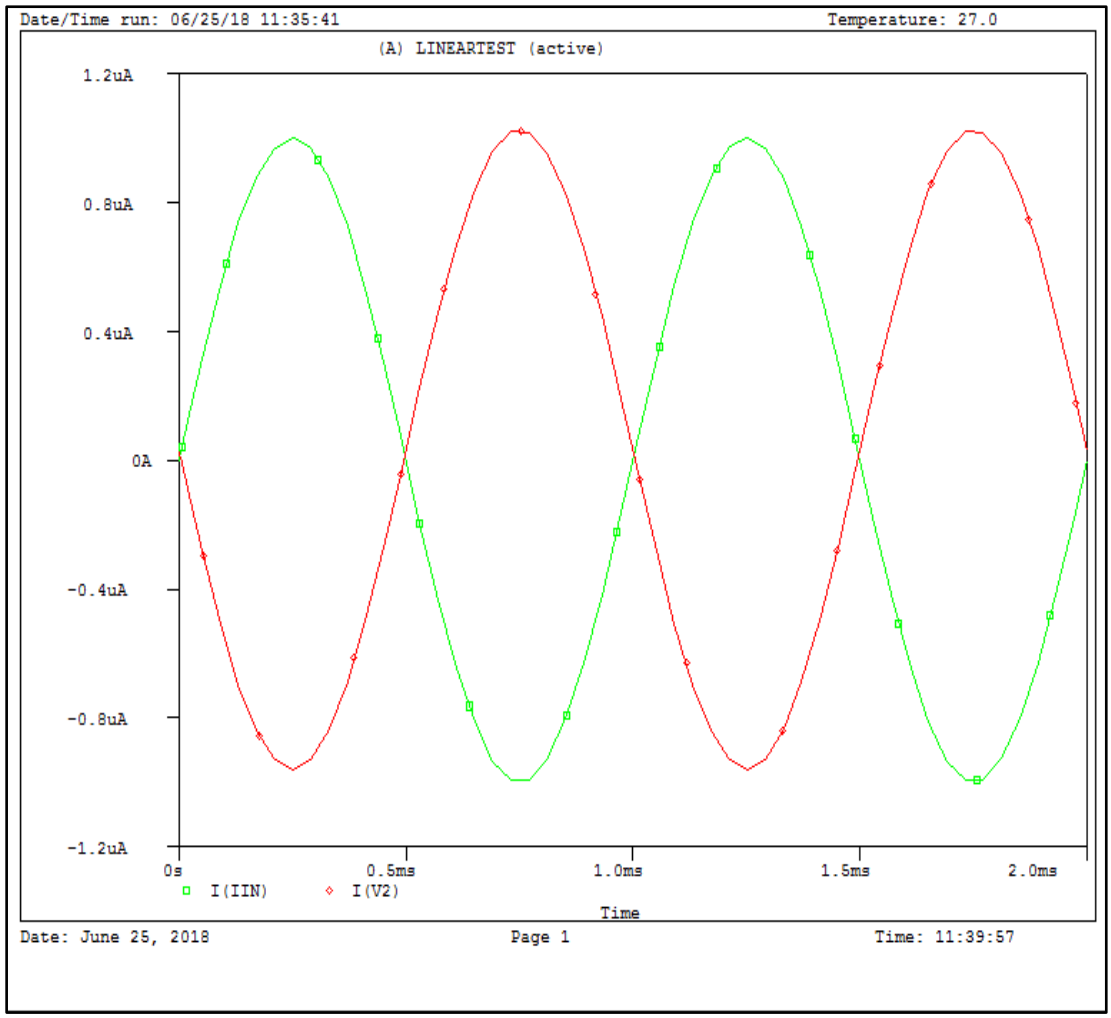

Fig 3.6 Transient Result for negative linear term generator

3.3.5 AC ANALYSIS OF LINEAR BLOCK

The AC analysis is performed in PSPICE A/D, using the same transistor models NR200N and PR200N of ALA400 transistor array from AT&T company, its magnitude versus frequency and phase versus frequency graph is shown below in Fig 3.7 and Fig 3.8 with the varying frequency 1KHz to 50KHz.

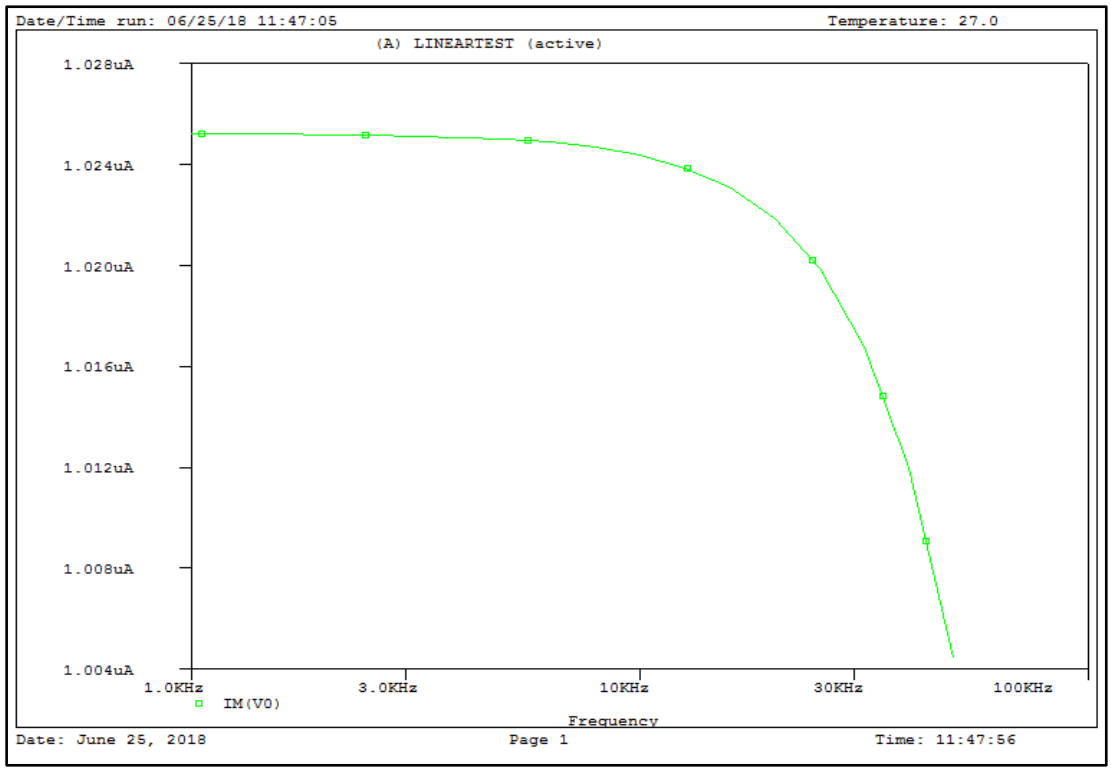

Fig 3.7 Gain magnitude versus frequency response for linear block

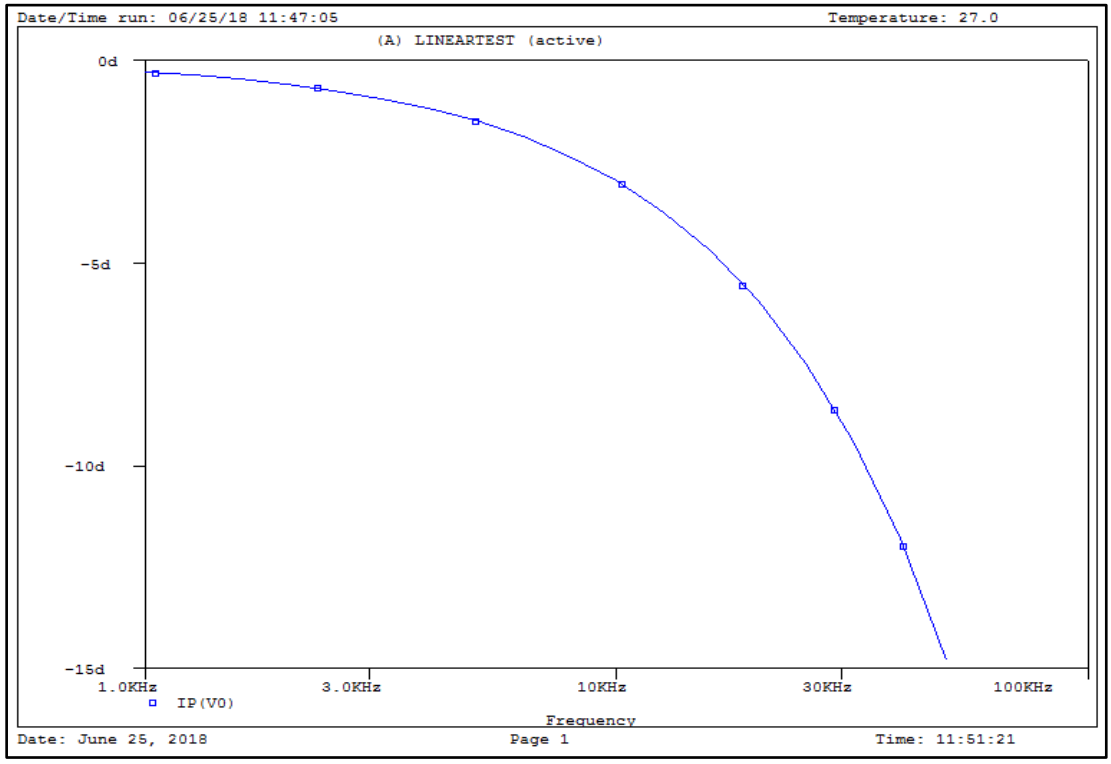

Fig 3.8 Phase angle versus frequency for linear block

It can be observed from the above Fig 3.7 that the gain of the linear block is nearly equal to unity for wide range of frequencies i.e. up to 10KHz.

3.3.6 COMPARITIVE ANALYSIS WITH IDEAL CHARACTERISTIC

This block's comparison is performed in MATLAB with ideal linear function behavior. The analysis between ideal and simulated results is shown by plotting the comparison graph as shown below in Fig 3.9, where blue line represents the simulated results and red line represents the ideal results. The maximum error for negative values of input is at input current signal of -10mA which is equal to 4% and maximum error for positive values of input is at input current signal of +10mA with value equal to 2%.

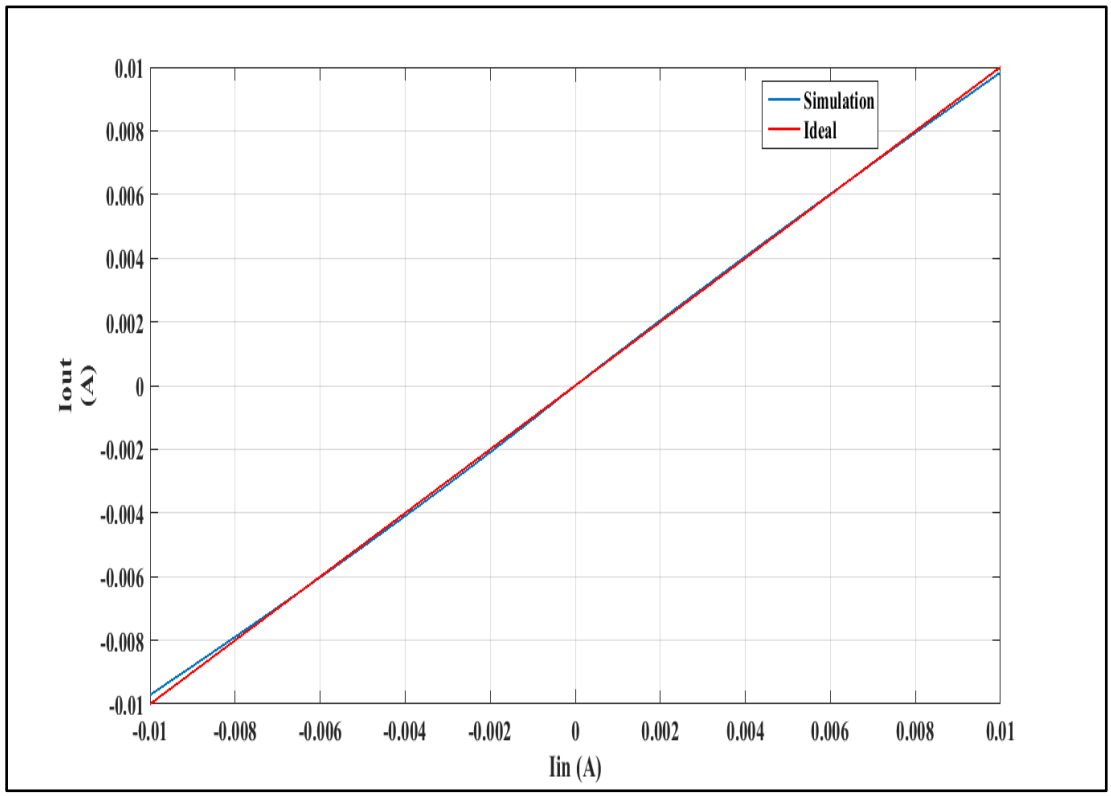

Fig 3.9 Comparison with Ideal Characteristics

3.4 SQUARE TERM GENERATOR/BLOCK

The second order term i.e. squarer term, which will be used in realizing the functions with Taylor series expansion in chapter 4, is generated and analyzed in this section. In this dissertation, the squarer term is realized using bipolar transistors and comparison with ideal behavior is also presented in this section.

This circuit is implemented using log-antilog blocks proposed in [5], this circuit is also based on translinear principle. The circuit diagram for square generator is shown in Fig 3.10 below with the derivation and results under this section.

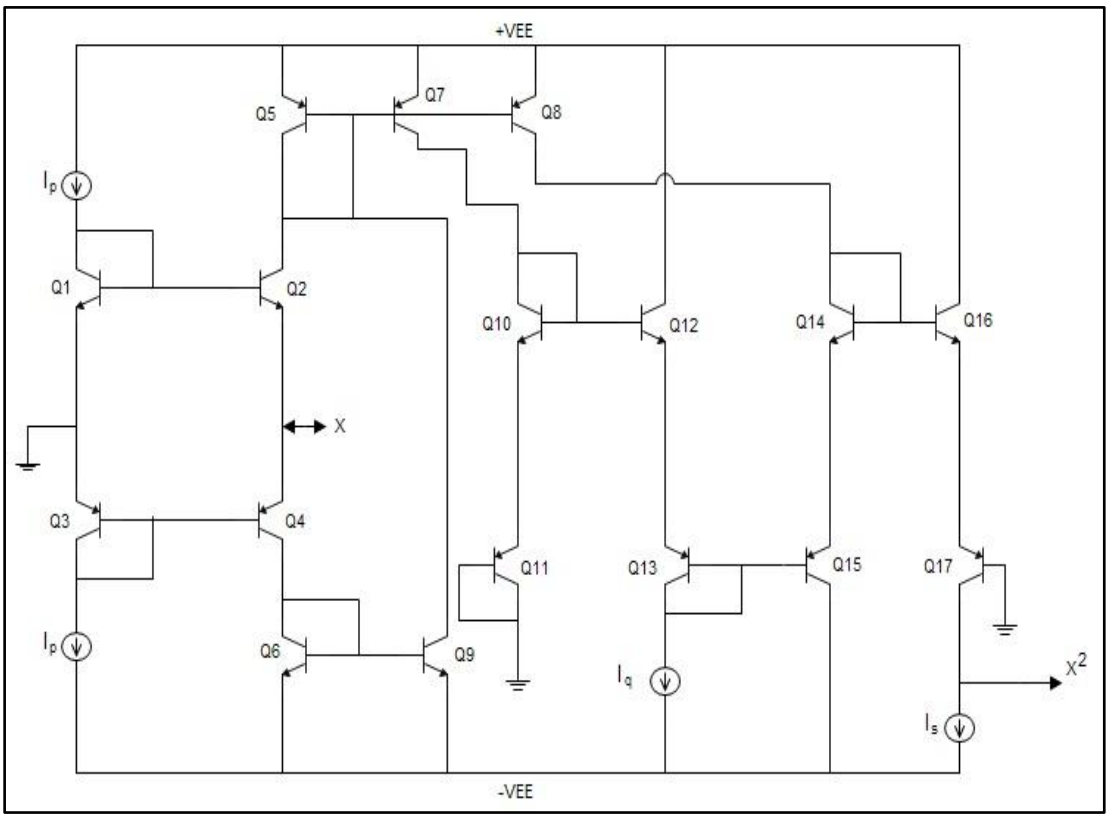

Fig 3.10 Square Term Generator Circuit

3.4.1 IDEAL ANALYSIS OF SQUARE TERM GENERATOR

Considering all the bipolar transistors to be ideal i.e. neglecting the effect of β, the above circuit shown in Fig 3.10 can be analyzed as below. From the translinear loop formed by Q1-Q4, we have:

$$V_{BE1} + V_{EB3} = V_{BE2} + V_{EB4} \tag{3.33}$$

Thus,

$$I_p I_p = I_{C2} I_{C4} \tag{3.34}$$

And,

$$I_{C4} = I_{C2} \pm X \tag{3.35}$$

Hence,

$$I_{C2} = \frac{\mp X \pm \sqrt{X^2 + 4I_p^2}}{2} \tag{3.36}$$

$$I_{C4} = \frac{\pm X \pm \sqrt{X^2 + 4I_p^2}}{2} \tag{3.37}$$

$$I_{C5} = I_{C2} + I_{C9} \tag{3.38}$$

And $I_{C9} = I_{C6} = I_{C4}$

Therefore,

$$I_{C5} = \pm\sqrt{X^2 + 4I_p^2} \tag{3.39}$$

And $I_{C7} = I_{C8} = I_{C5} = \pm\sqrt{X^2 + 4I_p^2}$

Now Q10-Q17 form a one quadrant analog multiplier [5], and its output can be derived from logarithmic and exponential block explained in chapter 2. Using those results expressed in equations 2.24 and 2.31, we get

$$V_{B13} = 2V_T \ln\left(\frac{I_{C10}}{I_q}\right) \quad (3.40)$$

And,

$$I_{C17} = I_{C14} exp\left(\frac{V_{B13}}{2V_T}\right) \quad (3.41)$$

Also,

$$I_{C10} = I_{C14} = \pm\sqrt{X^2 + 4I_p^2} \quad (3.42)$$

We have,

$$I_{out} = I_{C17} - I_S \quad (3.43)$$

Solving for equations 3.41 gives,

$$I_{out} = \frac{X^2+4I_p^2}{I_q} - I_s \quad (3.44)$$

Keeping $I_p = I_q = 1uA$ and $I_s = 4uA$, we get

$$I_{out} = X^2 \quad (3.45)$$

3.4.2 EXACT ANALYSIS OF SQUARE TERM GENERATOR/BLOCK

From above Fig 3.10, considering the effect of common-emitter gain β, the exact analysis can be done as follows:

$$V_{BE1} + V_{EB3} = V_{BE2} + V_{EB4} \quad (3.46)$$

Therefore,

$$I_{C1}I_{C3} = I_{C2}I_{C4} \quad (3.47)$$

Also,

$$I_p = I_{C1} + \frac{I_{C1}}{\beta_n} + \frac{I_{C2}}{\beta_n} \tag{3.48}$$

And,

$$I_p = I_{C3} + \frac{I_{C3}}{\beta_p} + \frac{I_{C3}}{\beta_p} \tag{3.49}$$

Also,

$$I_{E4} = I_{E2} \pm X \tag{3.50}$$

That is,

$$I_{C4} + \frac{I_{C4}}{\beta_p} = I_{C2} + \frac{I_{C2}}{\beta_n} \pm X \tag{3.51}$$

After solving equations we get I_{C2} and I_{C4} as follows in terms of β.

$$I_{C2} = \mp\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right]X \pm \frac{\beta_n\sqrt{X^2+4I_p^2}}{2(1+\beta_n)} \tag{3.52}$$

$$I_{C4} = \pm\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]X \pm \frac{\beta_p\sqrt{X^2+4I_p^2}}{2(1+\beta_p)} \tag{3.53}$$

$$I_{C5} = I_{C2} + I_{C9} \tag{3.54}$$

Therefore,

$$I_{C5} = \mp\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right]X \pm \frac{\beta_n\sqrt{X^2+4I_p^2}}{2(1+\beta_n)} + \left(1+\frac{2}{\beta_n}\right)\left(\pm\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]X \pm \frac{\beta_p\sqrt{X^2+4I_p^2}}{2(1+\beta_p)}\right) \quad (3.55)$$

And,

$$I_{C7} = I_{C8} \cong \pm\frac{1}{2}\left(1+\frac{2}{\beta_p}\right)\left[\frac{\beta_n}{1+\beta_n} + \frac{\beta_p}{1+\beta_p}\left(1+\frac{2}{\beta_n}\right)\right]\sqrt{X^2+4I_p^2} \quad (3.56)$$

Now considering the multiplier block Q10-Q17, Exact analysis follows the results as

$$V_{B13} = 2V_T \ln\left(\frac{I_{C7}-\frac{I_q}{1+\beta_n}}{I_q}\right) \quad (3.57)$$

And,

$$I_{C17} = \frac{\left(\frac{\beta_p}{1+\beta_p}\right)\frac{1}{I_q}I_{C7}^2 - \frac{\beta_p}{1+\beta_p}\frac{1}{(1+\beta_n)}I_{C7}}{1+\frac{I_{C7}}{I_q(1+\beta_n)} - \frac{1}{(1+\beta_n)^2}} \quad (3.58)$$

Since,

$$1+\beta_n \gg 1 \; and \; \left(1+\frac{2}{\beta_p}\right) \cong \left[\frac{1+\beta_n}{\beta_n}\right] \cong \left(1+\frac{2}{\beta_n}\right) \cong \left[\frac{1+\beta_p}{\beta_p}\right] \approx 1$$

We get,

$$I_{out} = \frac{\gamma\frac{X^2+4I_p^2}{I_q} \mp \alpha\sqrt{X^2+4I_p^2}}{1+\theta\sqrt{X^2+4I_p^2}} - I_s \quad (3.59)$$

Where $\gamma \approx 1;\ \alpha \ll 1;\ \theta \ll 1$

Therefore,

$$I_{out} \approx \gamma \frac{X^2+4I_p^2}{I_q} - I_s \tag{3.60}$$

Keeping $I_p = I_q = 1uA$ and $I_s = 4uA$, we get

$$I_{out} \approx \gamma X^2 + \rho \tag{3.61}$$

Where $\rho \ll 1$

The above equation 3.61 is derived while considering the effect of common-emitter gain for both pnp and npn bipolar transistors. The little bit deviation can be observed in the comparison plot with ideal characteristics below.

3.4.3 DC TRANSFER CHARACTERISTICS OF SQUARE TERM GENERATOR

The simulation has been performed in PSPICE A/D, with power supply voltage equal to ±3.65V, and $I_p = I_q = 1uA$ and $I_s = 4uA$, with the area of all transistors equal i.e. equal emitter width. The transistor models used for simulation are NR200N and PR200N. The DC characteristics for operating range of ± 15uA is simulated keeping the error within the realizable range as is shown below in Fig 3.11

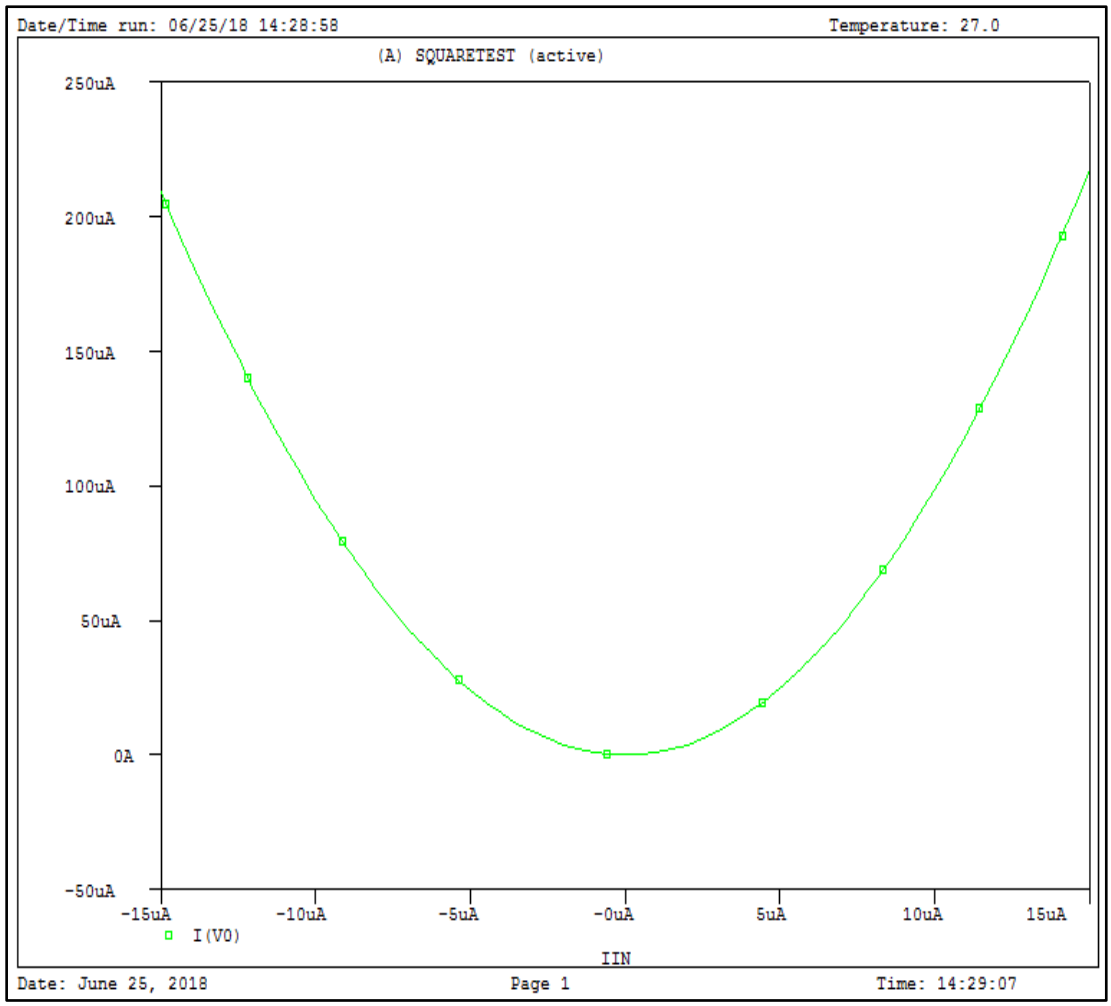

Fig 3.11 DC characteristics for square term generator/block

3.4.4 TRANSIENT ANALYSIS OF SQUARE BLOCK

The transient analysis of this block is shown in Fig 3.12 below, it is performed in PSPICE A/D, in which time is varying from 0ms to 2ms and applied input signal is in the form of sine wave with amplitude of 1uA and frequency of 1KHz.

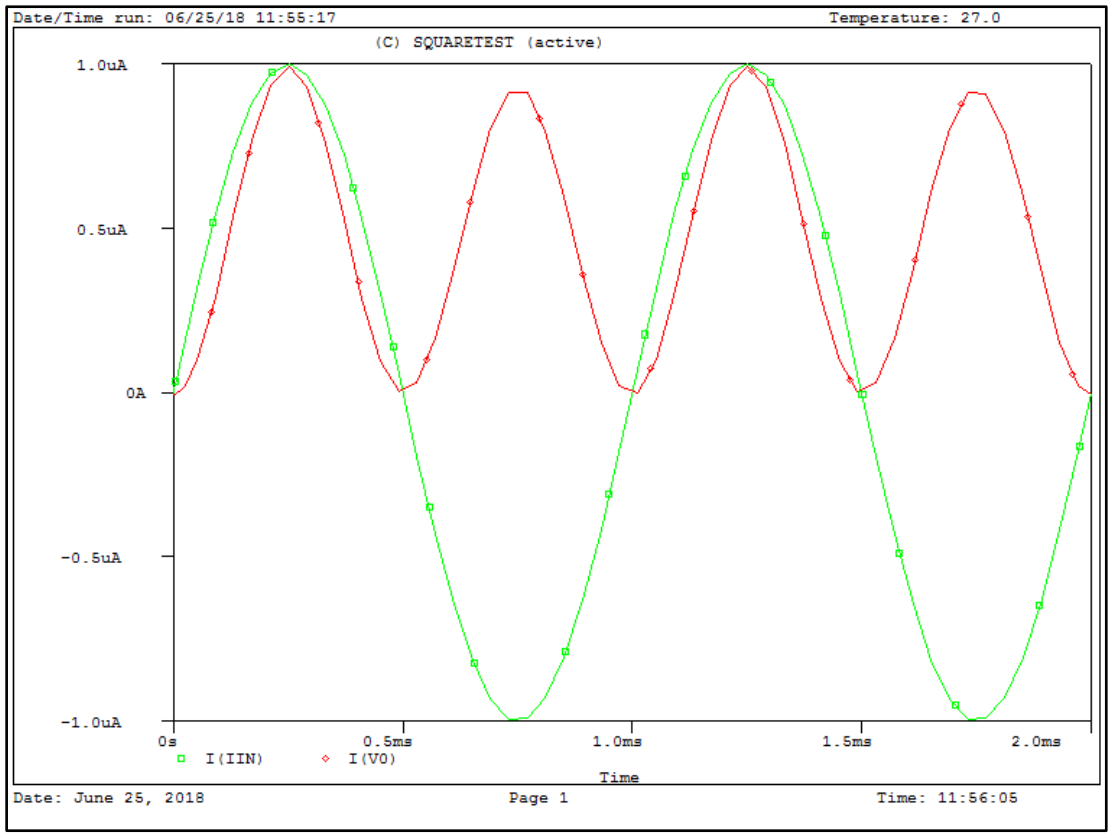

Fig 3.12 Transient analysis for square block

In the above graph red color shows the output of square block and green color graph shows the input signal. And it can be observed that the non-ideality is with small trade off in the output signal.

3.4.5 AC ANALYSIS OF SQUARE GENERATOR/BLOCK

The AC analysis is simulated in PSPICE A/D, with varying frequency from 1KHz to 10MHz as shown in Fig 3.13 and Fig 3.14 present the gain magnitude versus frequency and phase angle versus frequency graphs respectively.

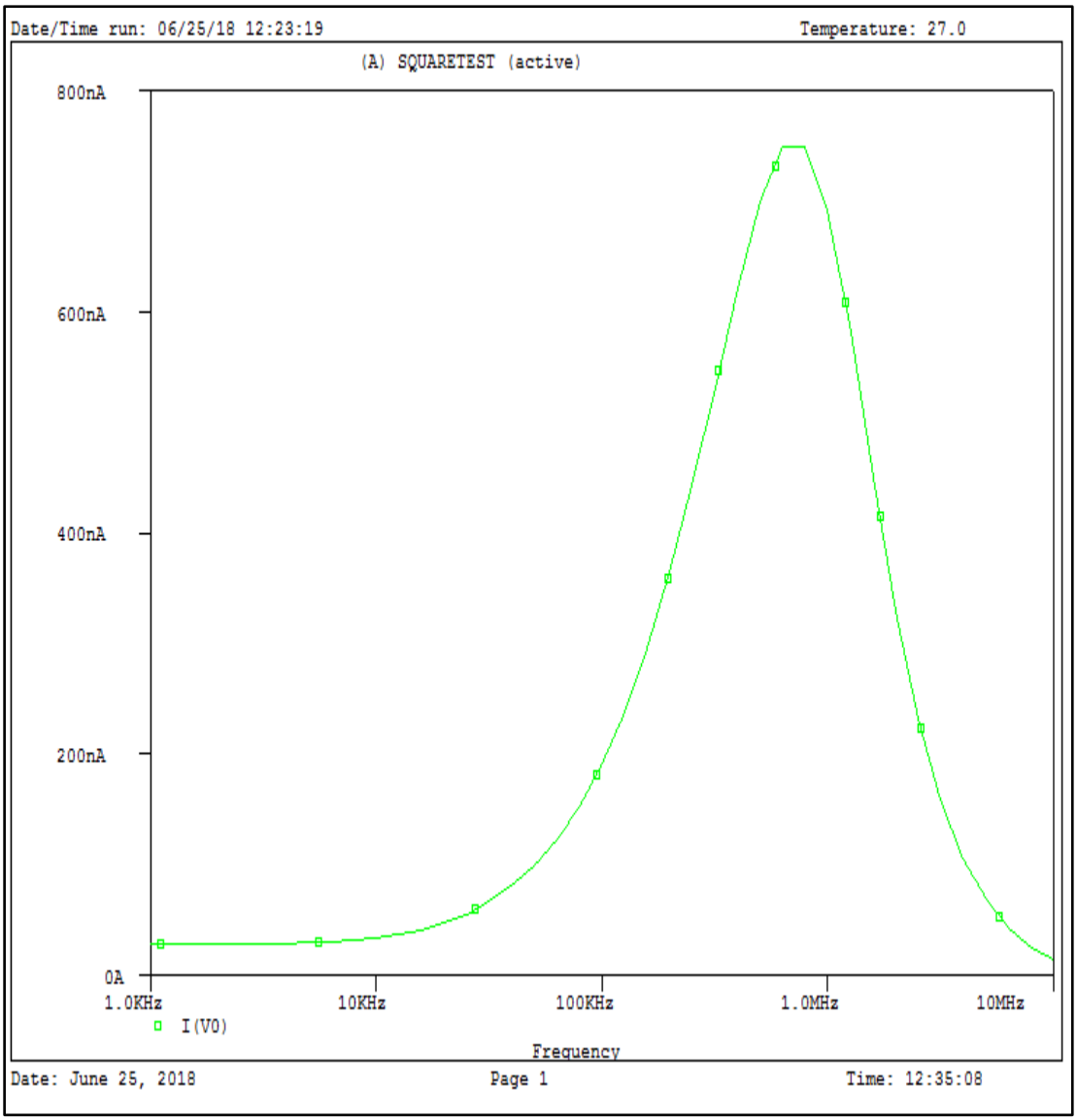

Fig 3.13 Gain Magnitude versus frequency for Square Block

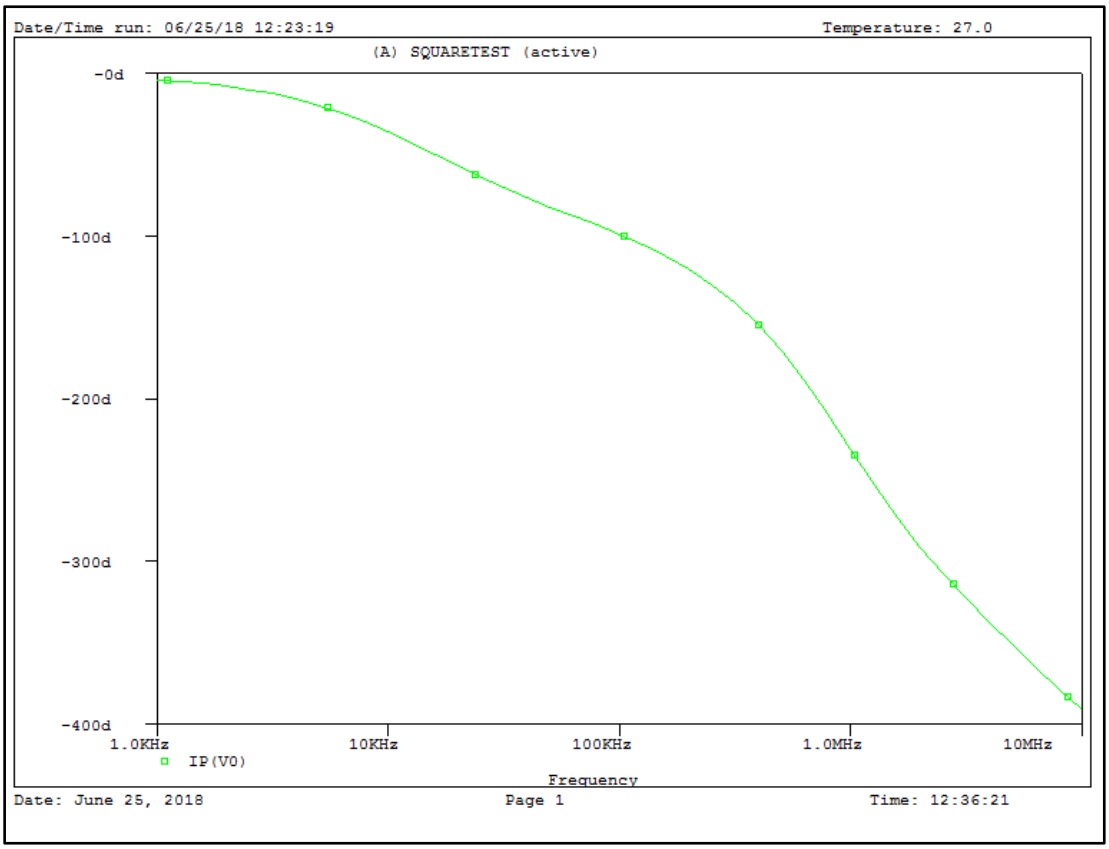

Fig 3.14 Phase angle versus frequency for Square Block

It can be observed from the above Fig 3.13 that unity gain is achieved at higher frequency and its unity gain bandwidth product is also high.

3.4.6 COMPARITIVE ANALYSIS WITH IDEAL SQUARE CHARACTERISTICS

This analysis is done in MATLAB, by plotting the graph between ideal results and simulated results of square term for the input current varying from -15uA to +15uA which are shown in red and blue color respectively shown in Fig 3.15 below.

It can be observed from the graph that maximum percentage error is at input value of -15uA which is 7.1% and minimum percentage error of 4% at input value of +15uA.

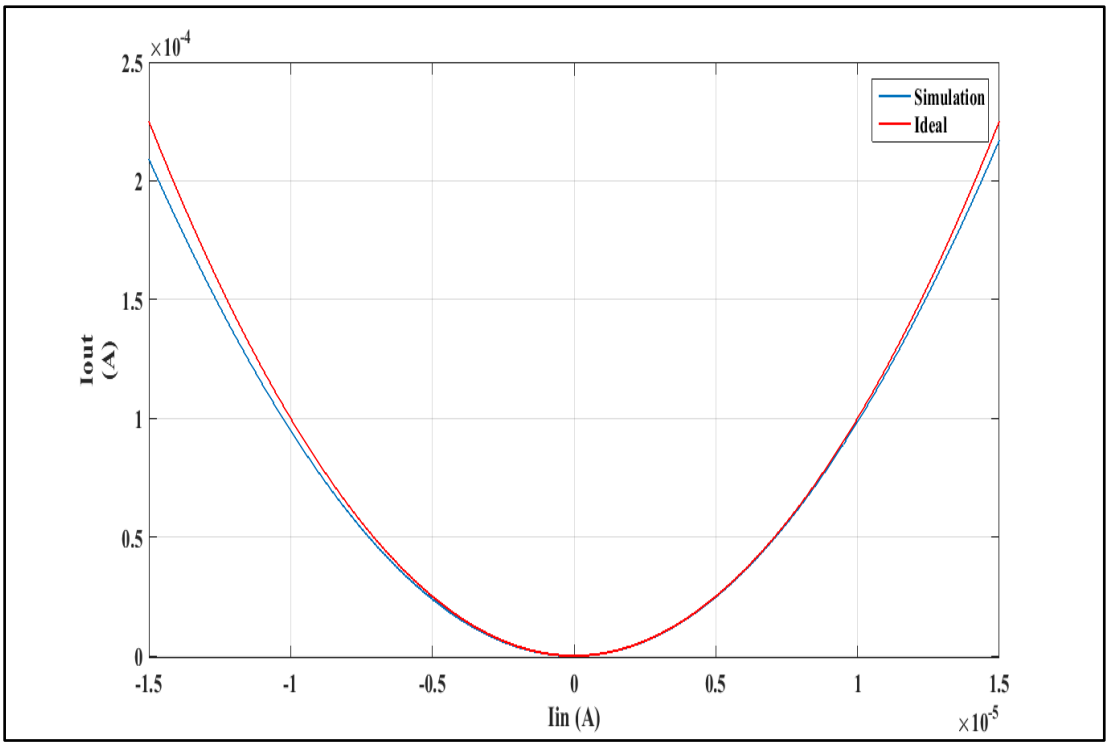

Fig 3.15 Comparison graph for square block with ideal characteristic

3.5 CUBIC TERM GENERATOR/BLOCK

With the generation of cubic term in current mode our approximation of functions discussed in chapter 4 reaches to more accurate realization. And also helps in analog implementation of elliptic curve which can be further used in security of networks.

Cubic term can be realized by simple mathematical manipulation shown in [6] as:

$$U = \left(\frac{V^2+V}{2}\right)^2 - \left(\frac{V^2-V}{2}\right)^2 = V^3 \tag{3.62}$$

The above simple manipulation can be realized with the help of above presented linear and squarer block. It can be noted from above equation 3.62 easily that addition and subtraction of terms is done at nodes, the positive linear term is used from the linear block and the negative linear term is used from the same linear term generator block as shown in Fig 3.3, It should be noted here that the linear term

is bidirectional hence it cannot be copied directly using current mirrors, but we have to use the linear block instead and also in order to keep our cubic term bidirectional we have to give input equal to square of current to last current mirrors used for subtraction to generate cubic term as shown in Fig 3.16, the scaling by the factor of four is done at the last stage of inverting current mirrors shown.

The scaling of cubic term plays a very important role while approximating the functions, since the functions that are approximated require scaled third order. Hence we have created a cubic block which generated the cubic and scaled terms of cube for further use in implementation of functions with the help of approximation. Here scaling is done at the stage where input to the current mirrors is in the form of square so that we can receive the output current in both directions without losing one directional current at the stage of current mirrors.

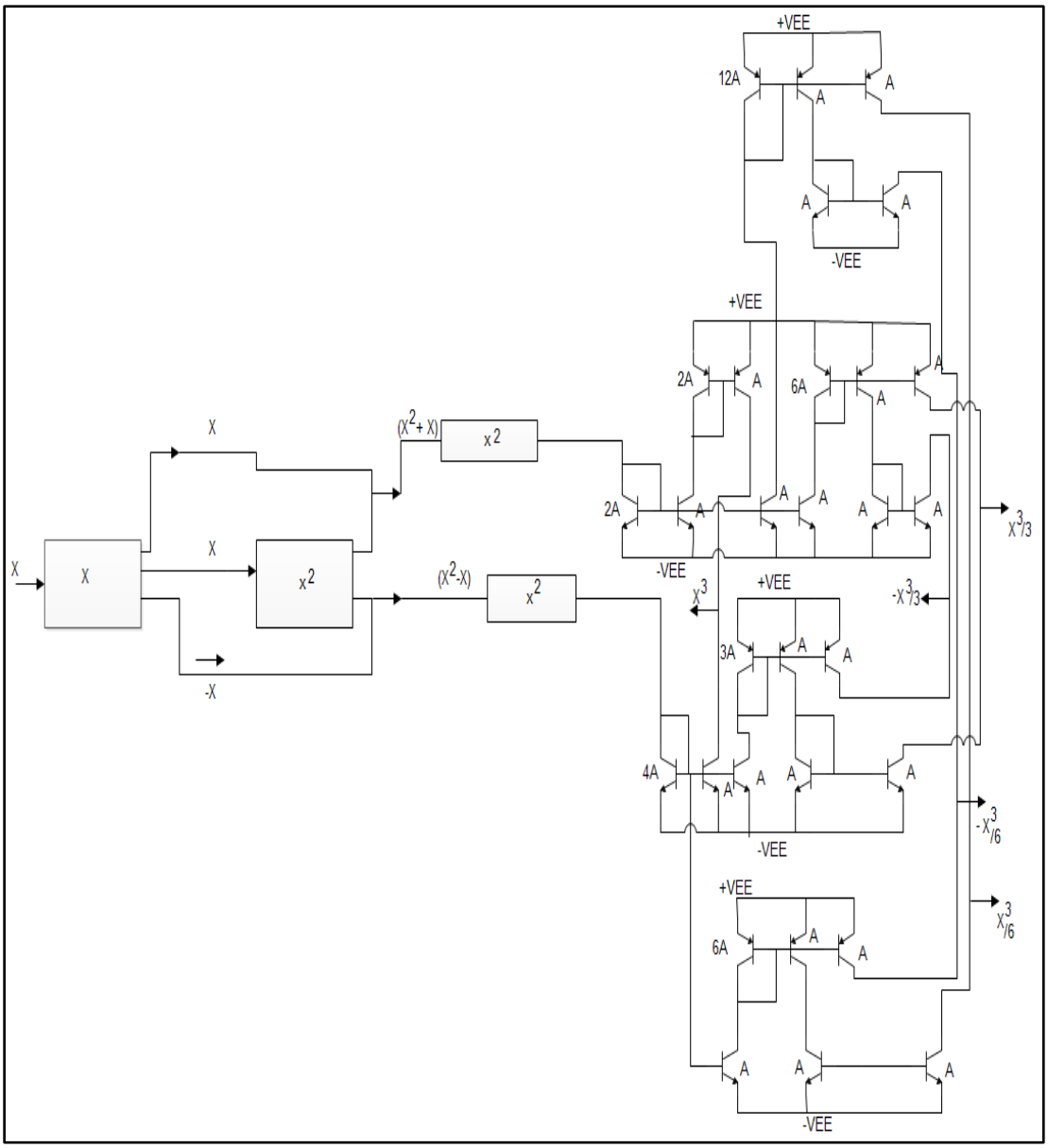

Fig 3.16 Cubic term generator Block

This circuit shown in Fig 3.16 contains more than 90 bipolar transistors hence it is shown in block diagram format, by creating sub circuits for linear and square blocks and which are used for generation of cubic term. It should be noted here that we have used inverting current mirror configuration at last stage with bipolar transistor's area twice which is actually developed in order to get scaled cubic term here by factor of 4. The block consists of scaled terms of cube which will

be further used for generation of functions. Complete block is represented in Fig 3.17 below.

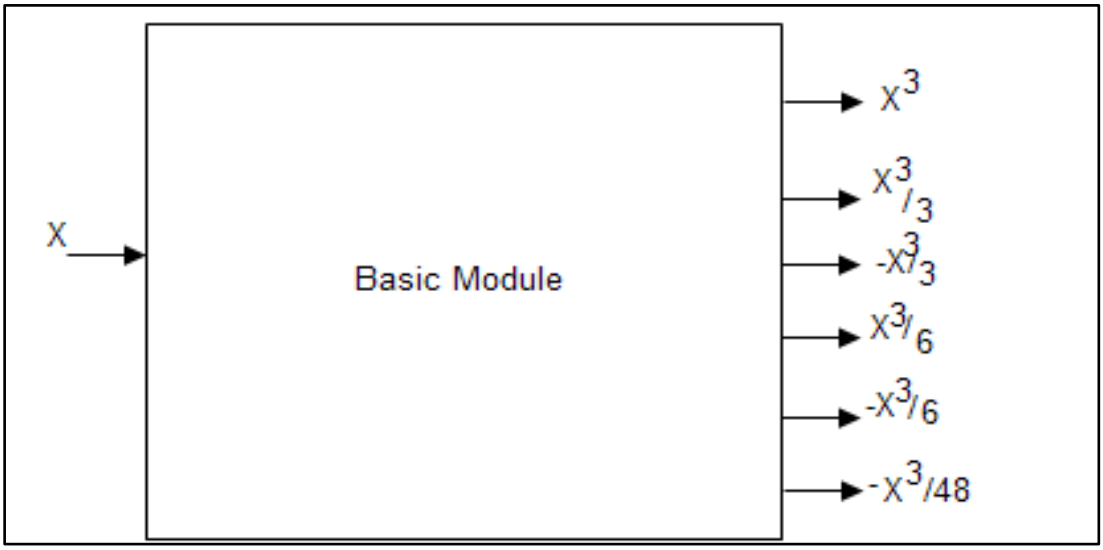

Fig 3.17 Block Diagram For cubic generator block

3.5.1 EXACT ANALYSIS OF CUBIC TERM GENERATOR

Circuit shown above in Fig 3.16 can be analyzed exactly by considering the effect of common-emitter gain i.e. β, since we have already gone through the tedious task of exact analyses of linear and square term in above section hence it becomes easy for us to derive the exact term for third order term with the help of exact approximation of linear and square terms respectively.

From equation 3.29 and 3.30 we have,

$$I_{linear\ -} = \mp\sigma X \; and \; I_{linear\ +} = \pm\varphi X \tag{3.63}$$

Where,

$$\sigma = \left(\left(1 + \frac{2}{\beta_p}\right)\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right] + \left(1 + \frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]\right) \approx 1$$

$$\varphi = \left(\left(1+\frac{2}{\beta_p}\right)\left(1+\frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_n}{1+\beta_n}\right] + \left(1+\frac{2}{\beta_p}\right)\left(1+\frac{2}{\beta_n}\right)\frac{1}{2}\left[\frac{\beta_p}{1+\beta_p}\right]\right) \approx 1$$

And from equation 3.61 we have,

$$I_{square} \approx \gamma X^2 + \rho \tag{3.64}$$

Where,

$$\gamma = \frac{\beta_p}{1+\beta_p} \approx 1 \; and \; \rho \ll 1$$

Solving the above block diagram Fig 3.16 we get

$$I_{cube} \approx \frac{\gamma(\sigma+\varphi)X^3}{2} + \frac{\rho(\varphi+\sigma)X}{2} \tag{3.65}$$

Note that actually σ < 1, which is approximated equal to 1, hence the above equation 3.65 becomes as,

$$I_{cube} \approx \mu X^3 + \emptyset X \tag{3.66}$$

Where $\mu \approx 1 \; and \; \emptyset \ll 1$

And the deviation in the cubic term can be observed in the analysis with the ideal plot shown in later section below.

3.5.2 DC TRANSFER CHARACTERISTICS OF CUBIC BLOCK

The DC transfer characteristic shown in Fig 3.18 of the cube block which is simulated in PSPICE A/D using transistor models NR200N and PR200N of ALA400 transistor from AT&T company, keeping power supply voltage equal to ±3.65V. The circuit is tested for ±4uA of input current signal.

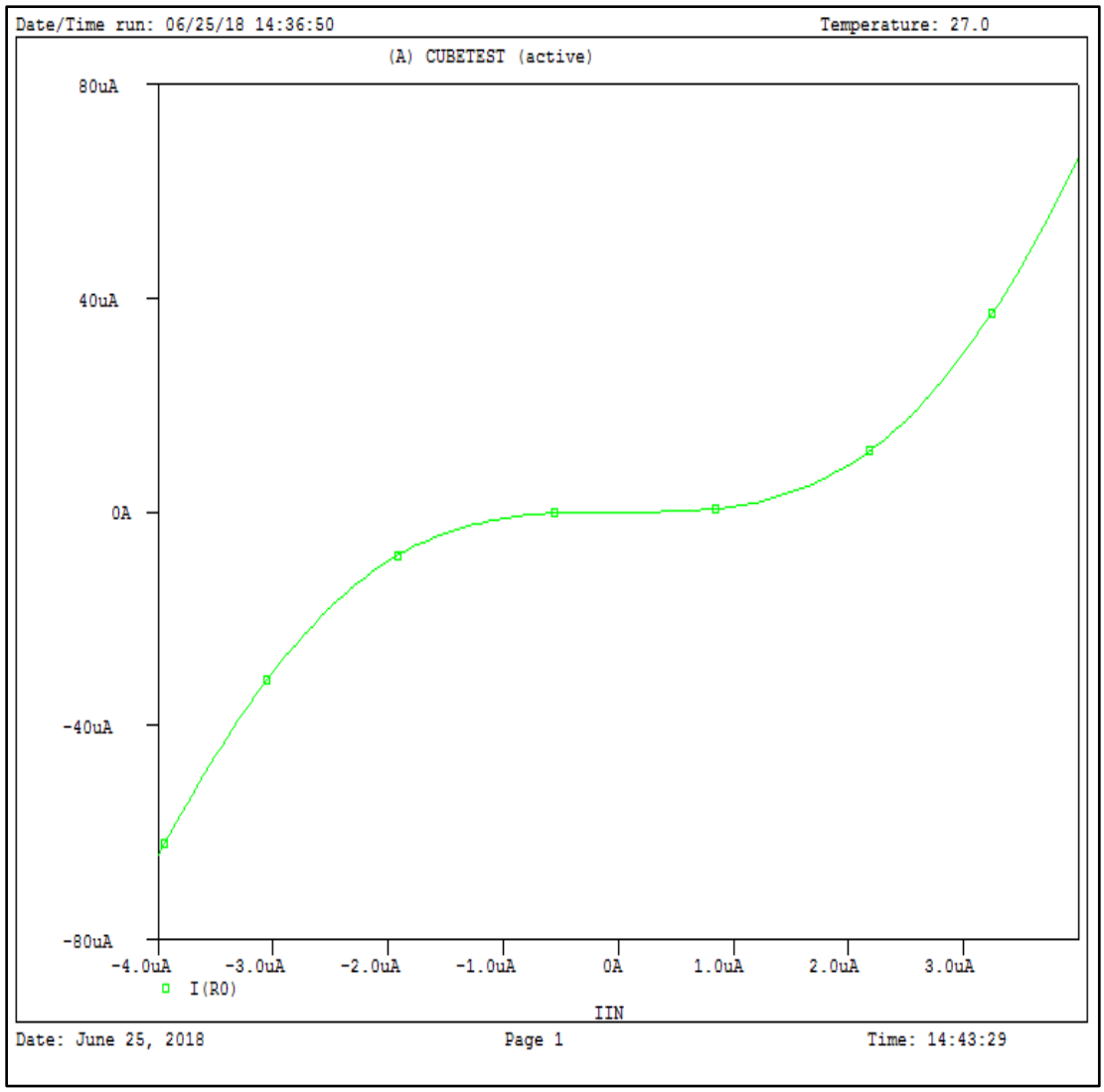

Fig 3.18 DC characteristic of Cube term generator

3.5.3 TRANSIENT ANALYSIS OF CUBIC GENERATOR/BLOCK

The transient analysis of this block is done in PSPICE A/D for 0ms to 2ms, with the input signal as sine wave with amplitude of 1uA at frequency 1KHz. The result of transient is shown in Fig 3.19 below.

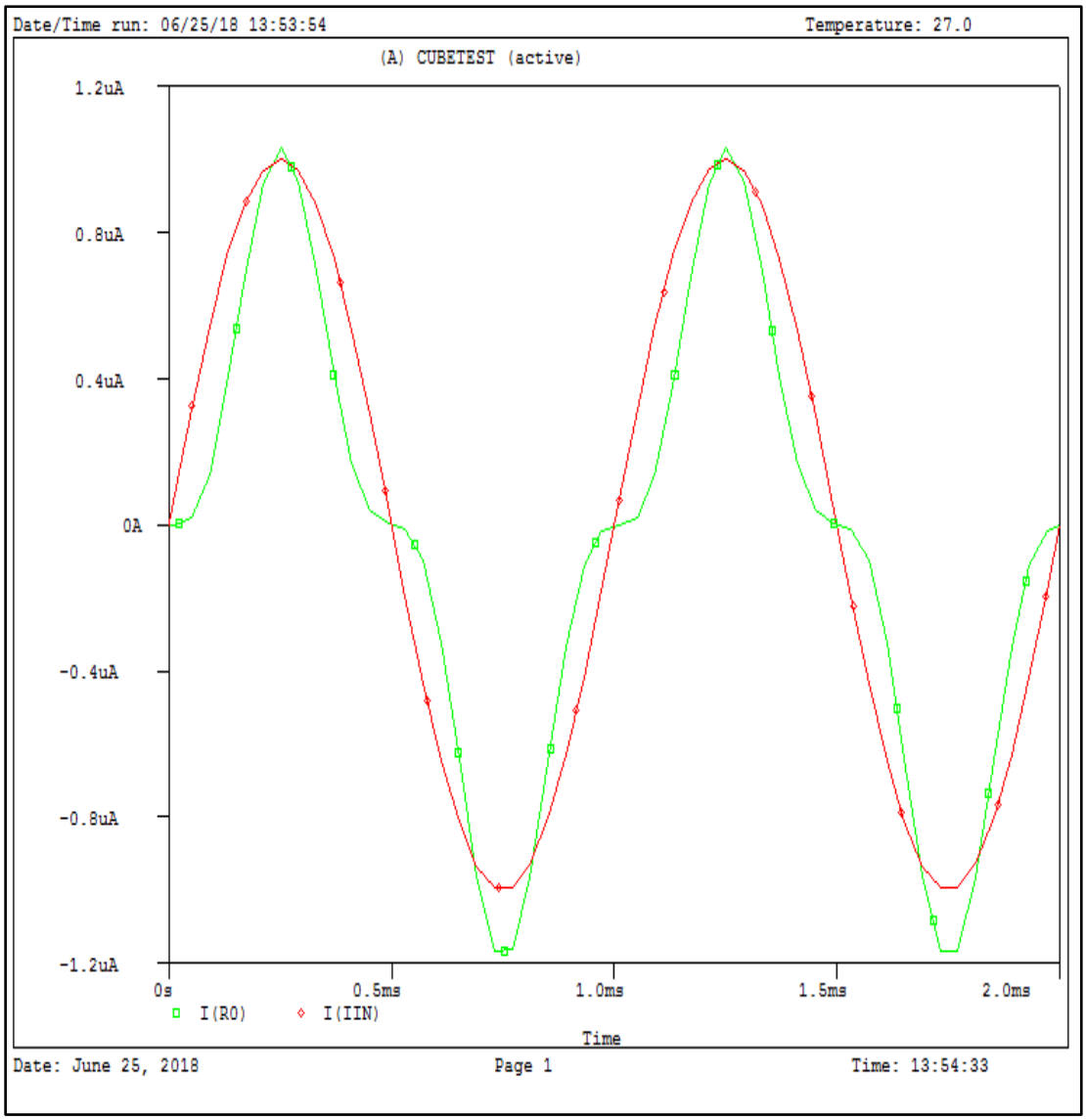

Fig 3.19 Transient response for Cube term generator/block

The non-ideality observed by doing exact analysis for cubic term is easily observable in fig 3.19.

3.5.4 AC ANALYSIS OF CUBIC GENERATOR/BLOCK

The AC analysis is done in PSPICE A/D by providing the input signal as sine wave with amplitude of 1uA and frequency 1KHz. The analysis provides the result for wide range of frequency ranging from 1KHz to 10MHz shown in Fig 3.20 and Fig 3.21 where Fig 3.20 provides us the gain magnitude versus frequency graph and Fig 3.21 provides us the phase angle versus frequency graph.

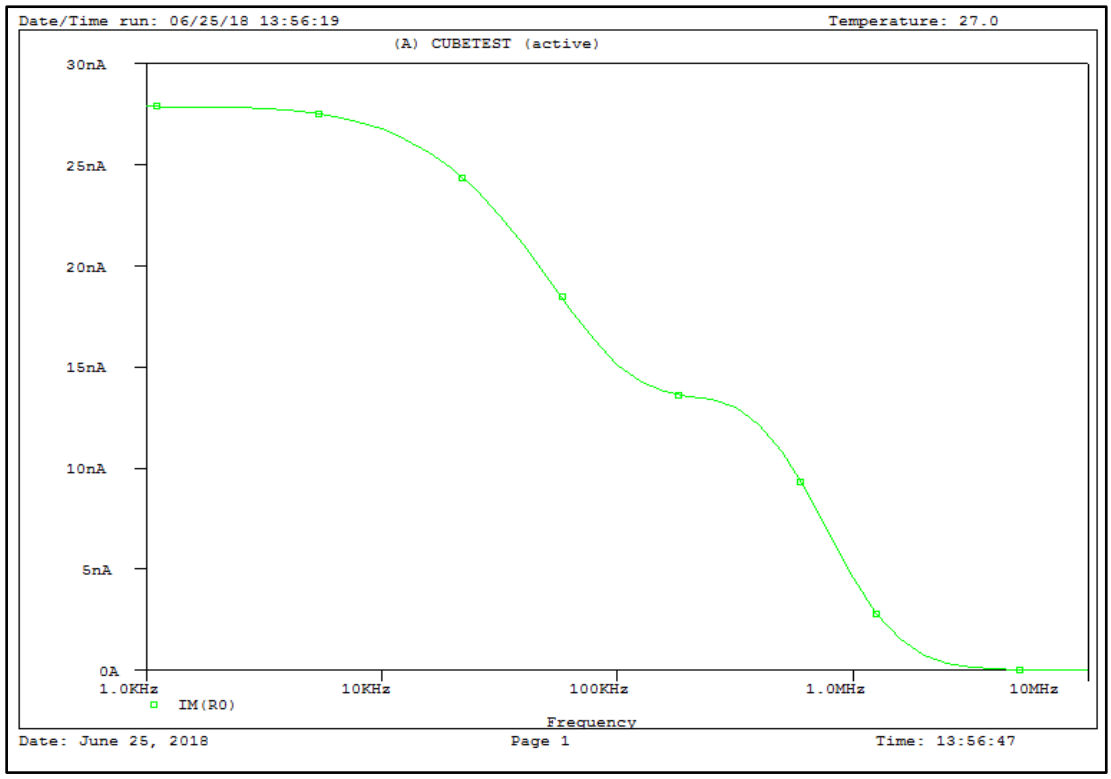

Fig 3.20 Gain magnitude versus frequency for Cubic generator

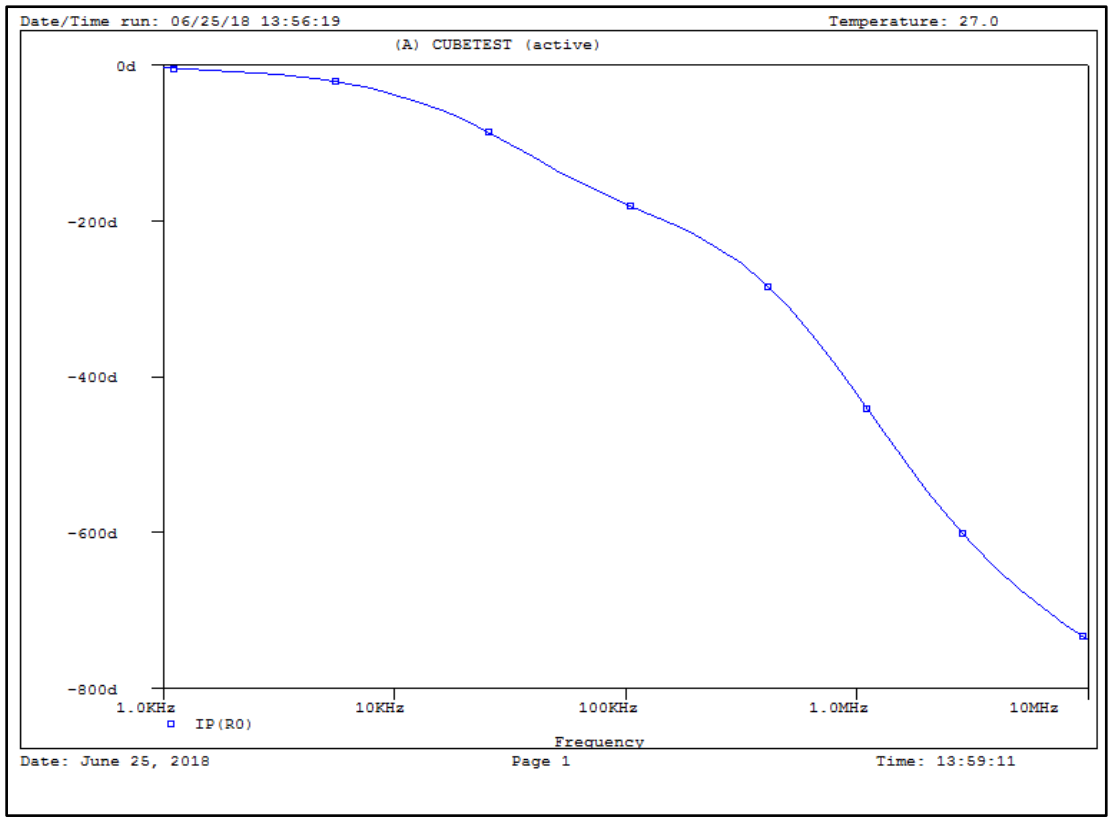

Fig 3.21 Phase angle versus frequency for cubic generator

The above graphs show us that the cubic generator circuits have good range of non distorted output for frequency up to 10KHz.

3.5.5 COMPARITIVE ANALYSIS WITH IDEAL BEHAVIOUR

The comparison between ideal and simulated behavior is shown in Fig 3.22, where our simulated cube generator circuit results in close values to the ideal values. The circuit has maximum error for negative range is 7.3% at input current of -3uA and for positive range, error is 4.46% at input current value equal to +3.3uA. The graph is plotted in MATLAB which is shown below. Here blue color graph shows the simulated where as red color graph shows the ideal behavior.

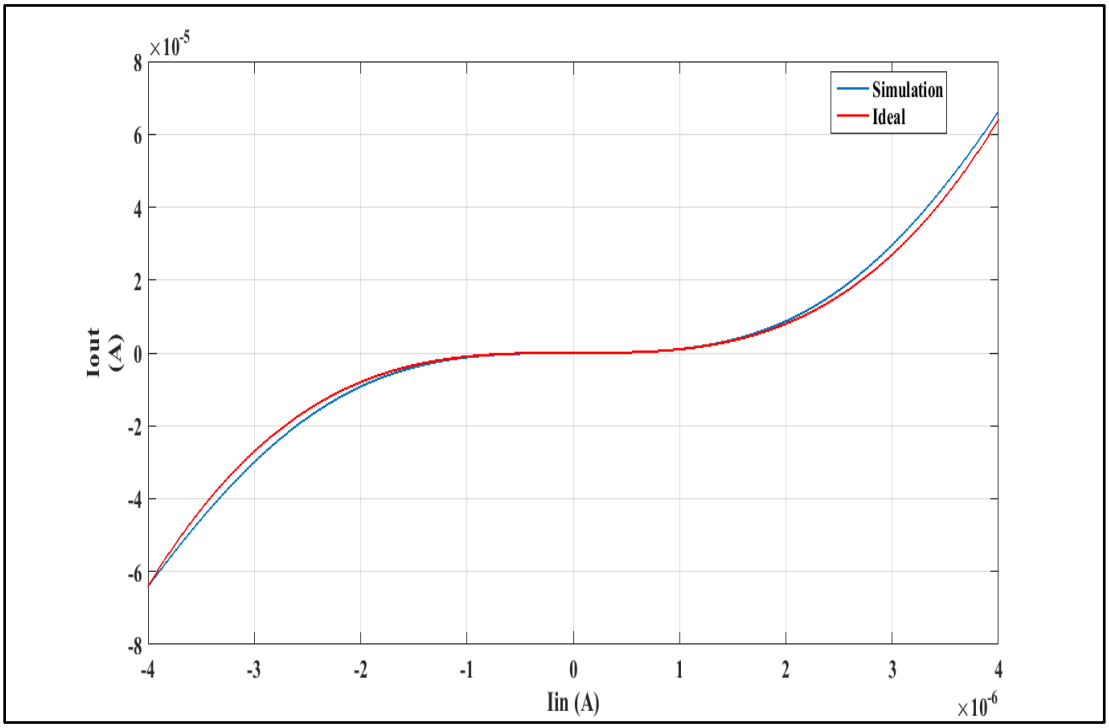

Fig 3.22 Comparison between Ideal and simulated results

3.6 FOURTH ORDER GENERATOR BLOCK

Our next block that will be frequently used while generating functions with the help of approximation method is the fourth order generating block, which gives the output equal to raise to power four to the input current. It consists of 34

bipolar transistors as shown in Fig 3.23. The circuit has been realized by cascading two square blocks. The equation for output is as follows:

$$I_{out} = I_{in}^4 \tag{3.67}$$

In the section below this circuit's Ideal behavior is analyzed and actual simulation results are compared with its ideal behavior.

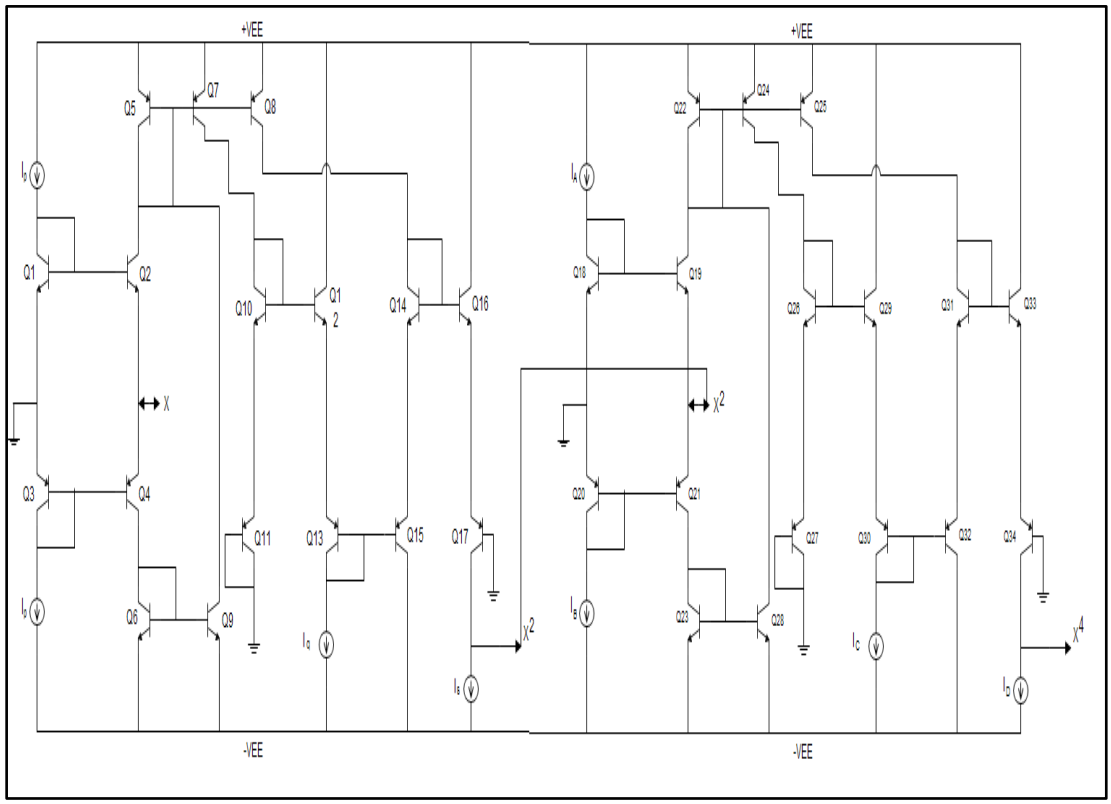

Fig 3.23 Fourth term generator circuit

3.6.1 DC TRANSFER CHARACTERISTICS OF FOURTH ORDER GENERATOR BLOCK

The DC transfer characteristics of this block is simulated in PSPICE A/D using the bipolar transistor model parameters of NR200N and PR200N of ALA400 transistor array from AT&T company. Circuit is simulated from input current ranging from -2uA to +2uA. Power supply voltage is kept same at ±3.65V. Current

sources value are $I_A = I_B = I_C = I_p = I_q = 1uA$ and $I_s = I_D = 4uA$. The simulated result is shown in Fig 3.24 below.

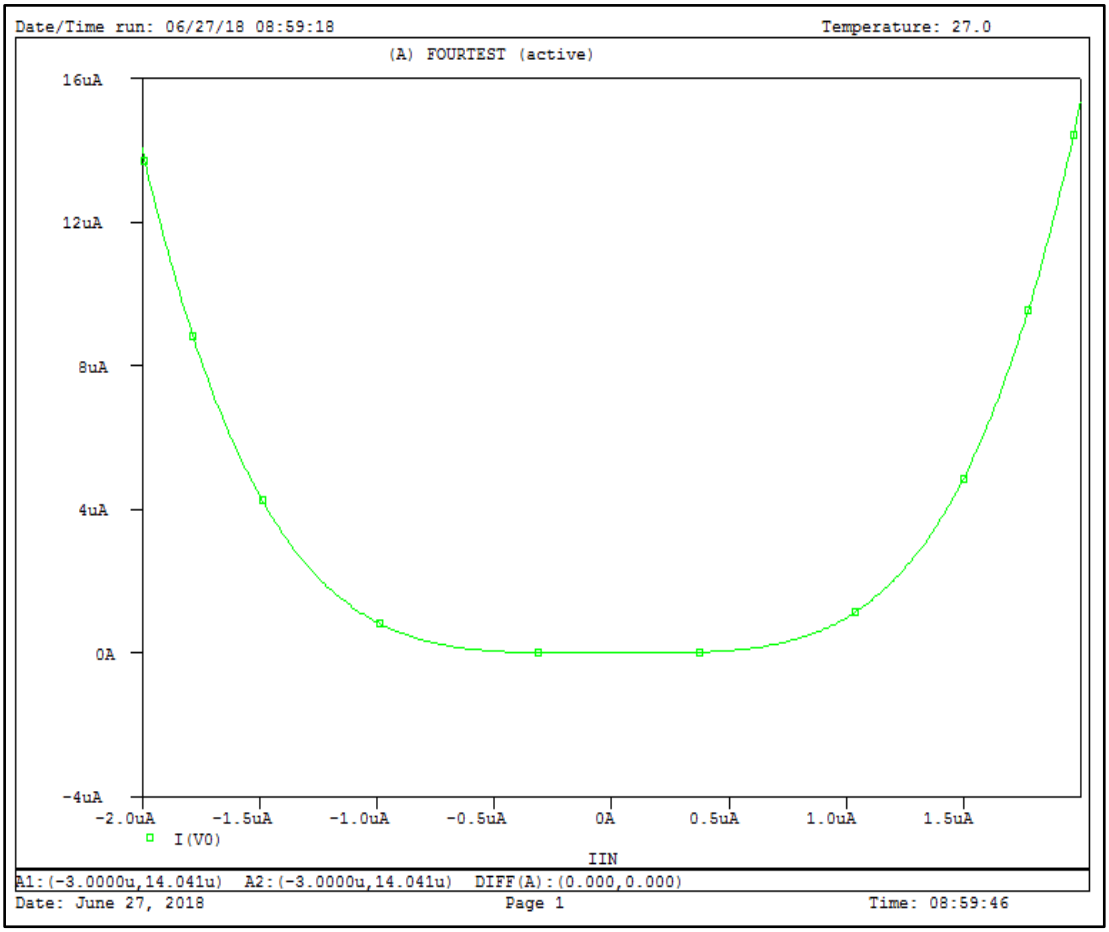

Fig 3.24 DC transfer characteristics for fourth term generator

3.6.2 TRANSIENT ANALYSIS FOR FOURTH TERM GENERATOR

Transient analysis is done in PSPICE A/D, with the input signal as sine wave with amplitude of 1uA, with frequency equal to 1KHz. The result is shown in Fig 3.25 below.

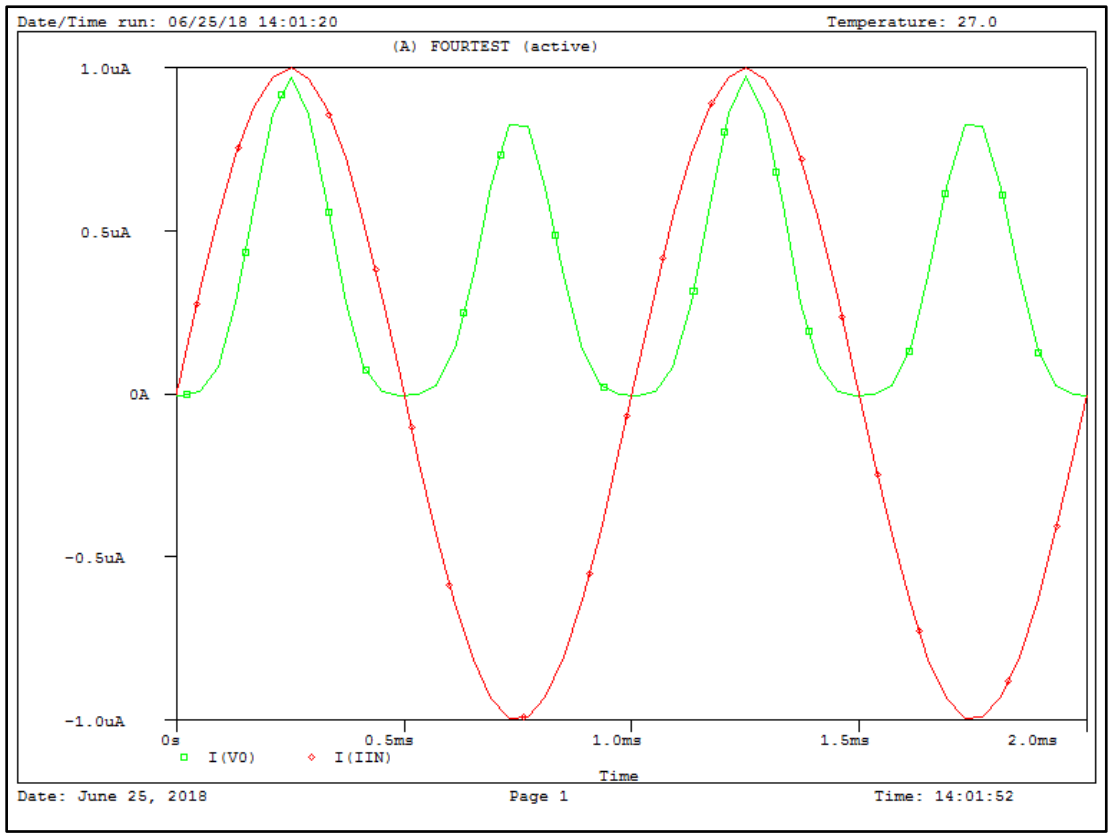

Fig 3.25 Transient response for Fourth term generator/block

3.6.3 AC ANALYSIS FOR FOURTH TERM GENERATOR/BLOCK

The AC analysis is done in PSPICE A/D using the same transistor model and keeping input signal as sine wave with 1uA amplitude and frequency 1KHz, the output is observed for wide range of frequency from 1KHz to 10MHz.

The gain magnitude versus frequency and phase angle versus frequency plot is shown in Fig 3.26 and Fig 3.27 below.

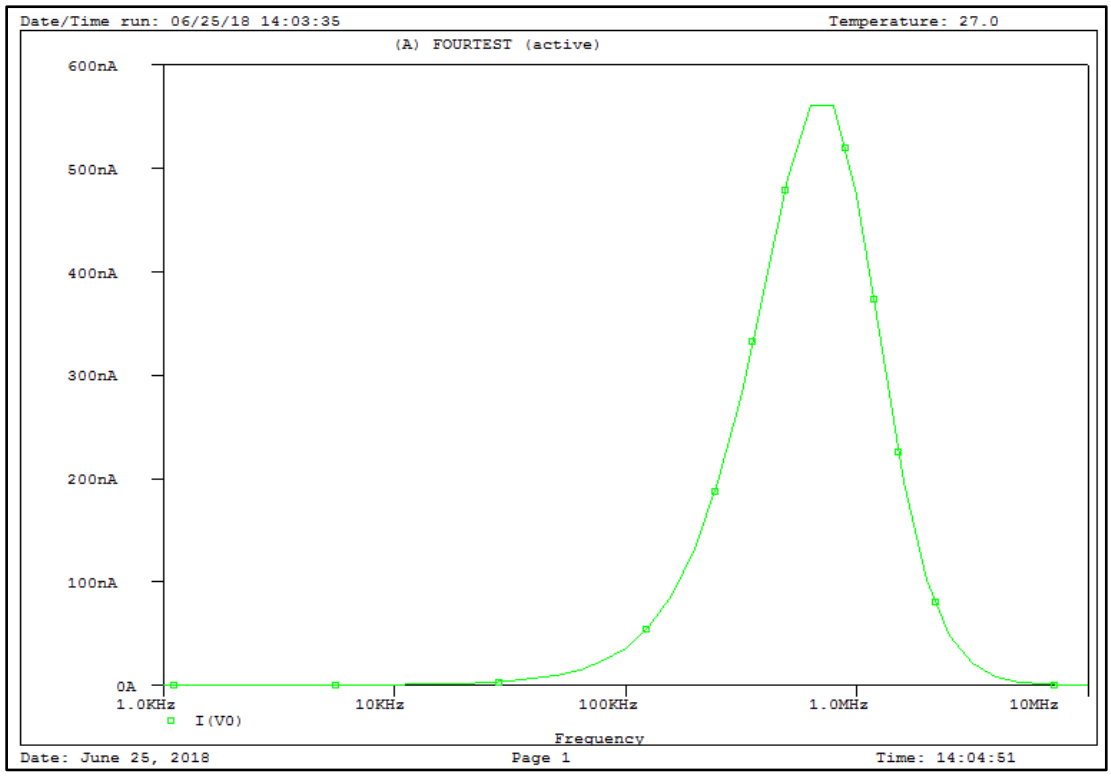

Fig 3.26 Gain Magnitude versus frequency graph for fourth term generator/block

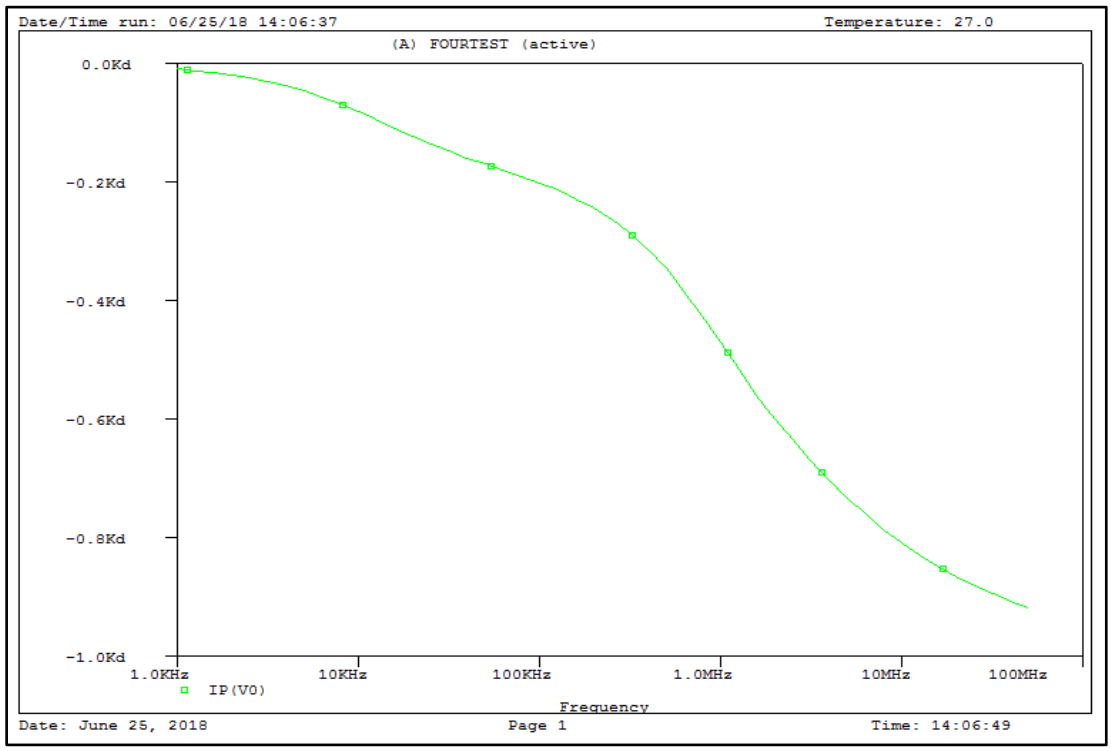

Fig 3.27 Phase angle versus frequency graph for fourth term generator/block

3.6.4 COMPARITIVE ANALYSIS FOURTH ORDER TERM GENERATOR WITH IDEAL CHARACTERISTICS

The comparison is done in MATLAB for the same input range varying from -2uA to +2uA for which this block has been simulated in PSPICE A/D. The ideal and simulated result is shown below in Fig 3.28 and it is calculated that maximum percentage of error is 10.3% at -2uA of input current signal and 3.89% at +2uA of input current signal. The simulated result is shown with blue color graph and ideal result with red color graph in Fig 3.8.

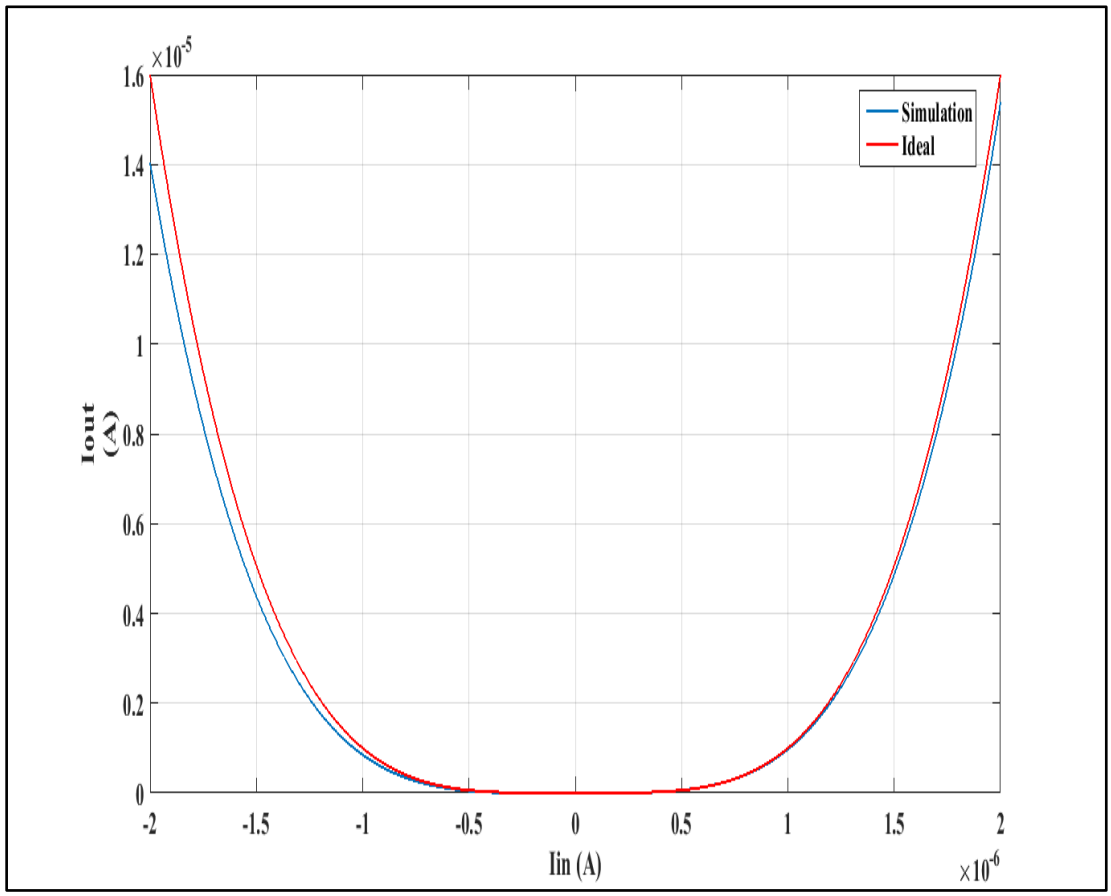

Fig 3.28 Comparison graph between Simulated and Ideal values for fourth order term

3.7 FIFTH ORDER TERM GENERATOR/BLOCK

This block generates the raise to power five of input current signal at its output terminal. This circuit has more than 100 bipolar transistors, because of this reason the circuit diagram of this block as shown is in block diagram form. Fifth order term can be generated with the help of little manipulation of equation 3.64 represented as follows

$$I_{out} = (I_{in}^3 + I_{in}^2)^2 - (I_{in}^3 - I_{in}^2)^2 = 4I_{in}^5 \quad (3.68)$$

The circuit realized has scaling factor of four with the help of inverting and non inverting current mirrors in order to give only raise to power five term. The circuit is shown in Fig 3.29 below.

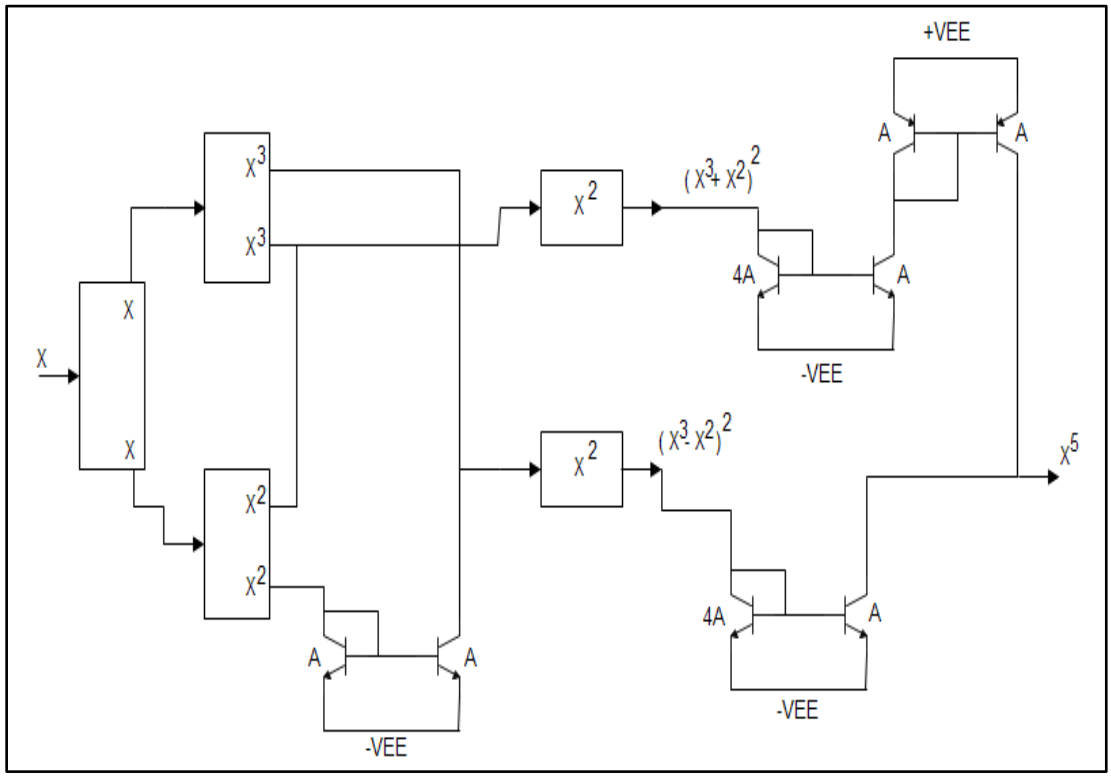

Fig 3.29 Fifth Order Generator/Block

3.7.1 DC TRANSFER CHARACTERSTICS OF FIFTH ORDER GENERATOR/BLOCK

The DC transfer characteristics of this block is simulated in PSPICE A/D using bipolar transistors model NR200N and PR200N of ALA400 transistor array from AT&T company. It is traced for input range varying from -1uA to +1uA and keeping the power supply equal to ±3.65V. This DC characteristic is shown in Fig 3.30 below.

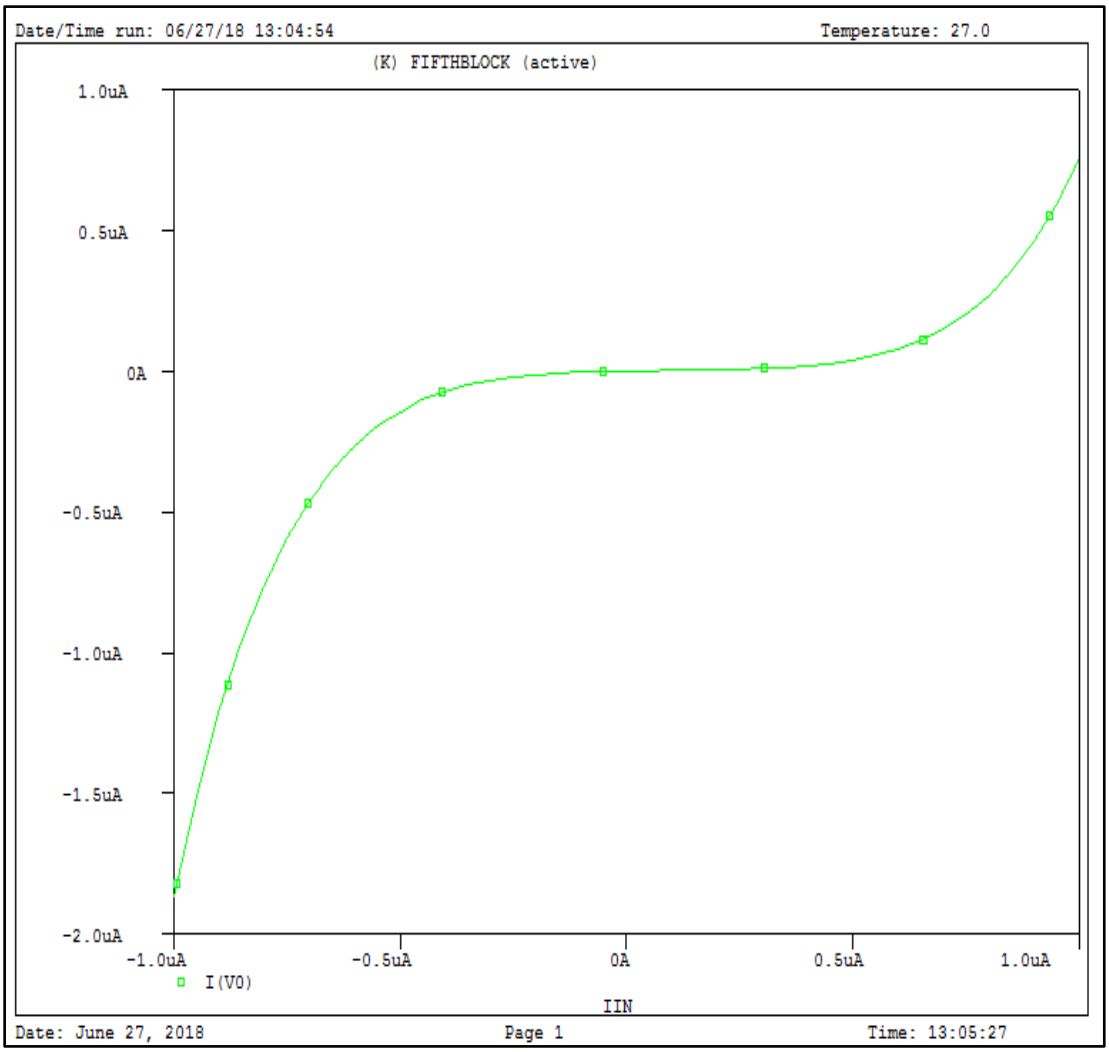

Fig 3.30 DC characteristics for fifth order term generator

3.7.2 TRANSIENT ANALYSIS OF FIFTH ORDER GENERATOR/BLOCK

The transient analysis is done in PSPICE A/D, with the input signal as sine wave with amplitude of 1uA and frequency 1KHz. The analysis is shown in Fig 3.31 below for 2ms with step size of 50us.

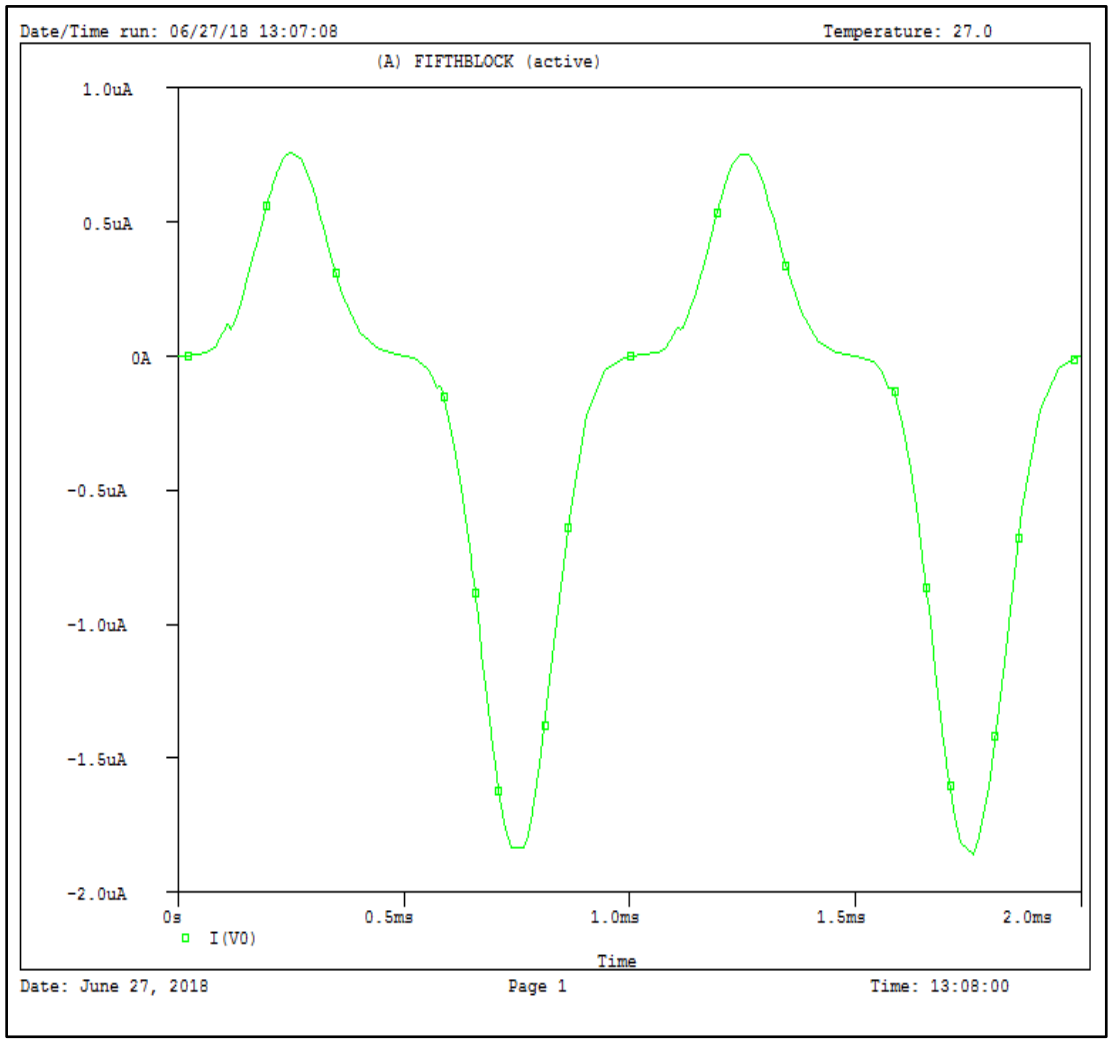

Fig 3.31Transient analysis of fifth order block

3.7.3 AC ANALYSIS OF FIFTH ORDER GENERATOR/BLOCK

The AC analysis is done in PSPICE A/D as shown in Fig 3.32 and Fig 3.33 below. The analysis is done by varying the frequency from 1KHz to 10MHz with step size of 10 decade and tracing the gain magnitude and phase angle for varying frequency. Input signal given to the circuit is sine wave with amplitude 1uA.

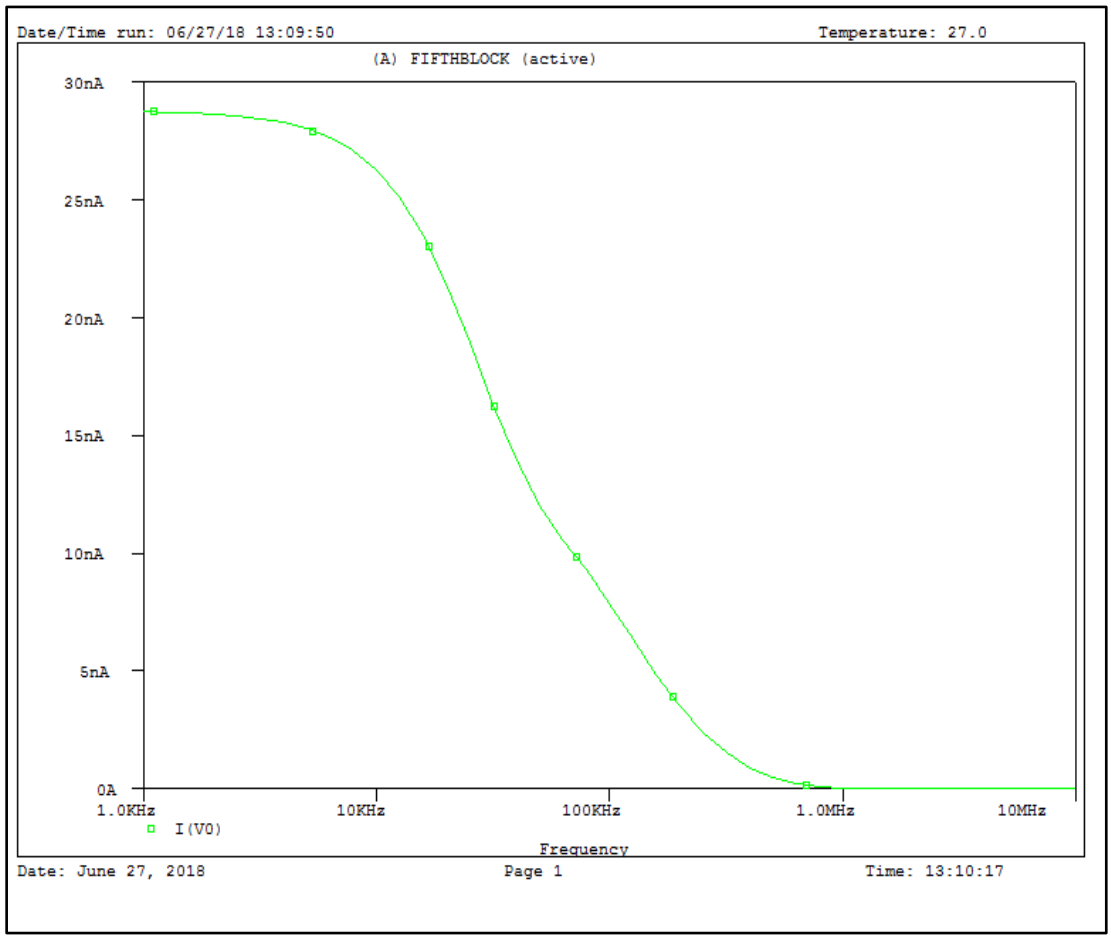

Fig 3.32 Gain magnitude versus frequency for fith order block

It is easily observable from the above Fig 3.32 that gain magnitude starts falling after 5KHz, providing a small range of operation. After this value distortion in the results will be observed for higher range of frequencies.

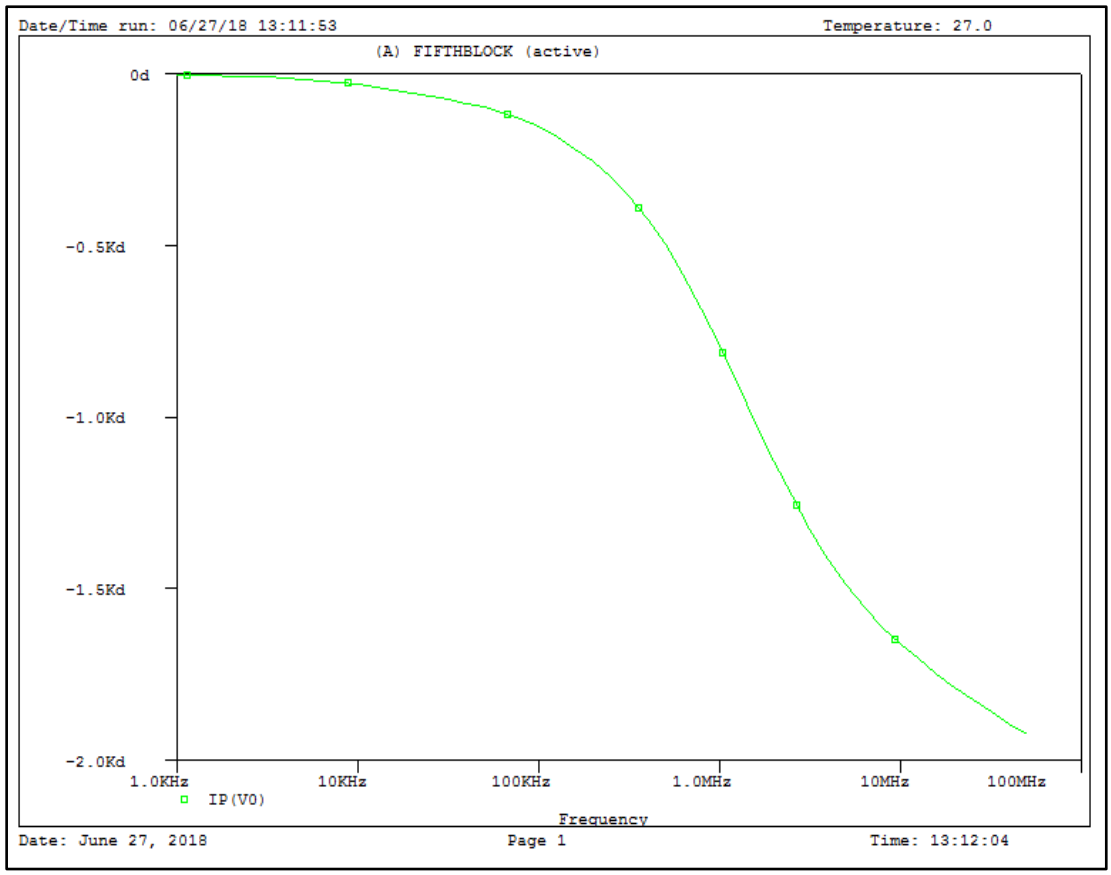

Fig 3.33 Phase angle versus frequency for Fifth order block

3.7.4 COMPARISON WITH IDEAL CHARACTERISTIC FOR FIFTH ORDER TERM

The non ideality in the above fifth order block will be observed when we trace a plot between simulated and ideal values which is represented in Fig 3.34 below. The plot has been traced in MATLAB using simulated data points and theoretical data points. Blue color plot indicates the simulated result and red color plot indicates the ideal result.

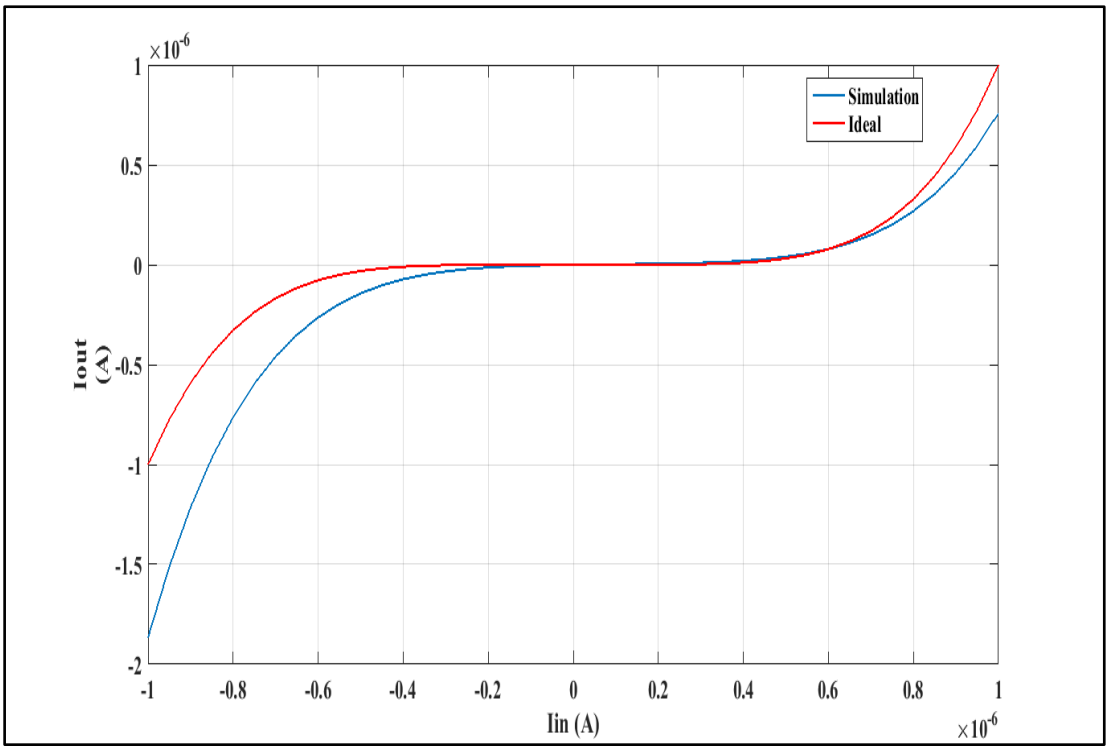

Fig 3.34 Comparison between Ideal and Simulated result for fifth order term generator

As we realized the fifth order term, the non ideality increases because of the common-emitter gain comes significantly into the effect. The error is maximum at input current signal value equal to -1uA but this block has ideally close behavior for small range of input current signal.

3.8 CONCLUSION

In this chapter we have realized the basic modules up to the order of five for approximation of functions which are implemented in chapter 4.

REFERENCES

[1] A. S. Sedra, K.C. Smith, Microelectronic circuits Theory and Applications, eds.6,2013,OxfordUniversityPress.

[2] A. N. Saatlo, S. Ozoguz, S. Minaei, "Applications of a CMOS Current Squaring Circuit in Analog Signal Processing," *IEEE Int. Conf. on Telecommunications and Signal Processing*,2015,pp.978-1-4799-8498-5.

[3] A.S. Sedra, G.W. Robert, "Current Conveyor Theory and Practice," *Analogue IC Design: The Current-Mode Approach*,London,1990,Chap. 3.

[4] B. Gilbert,"Translinear circuits: a proposed classification," *Electronics Letters*,vol.11,no.1,pp.14-16,1975.

[5] R. Groza, L. Festila, E. Szopos, "Four Quadrant Log-Domain Analog Current Multiplier," *IEEE Int. Conf. on Automation, Quality and Testing, Robotics*, Cluj-Napoca,Romania,2008,pp.1-4244-2577-8/08.

[6] M.T. Abuelma'atti, "Universal CMOS Current-Mode Analog Function Synthesizer," *IEEE Trans. On Circuits and Systems-I: Fundamental Theory andApplications*,vol.-49,no.-10,2002.

[7] M.H. Rashid, Introduction to PSpice Using OrCAD for Circuits and Electronics, eds. III, Pearson, 2004.

CHAPTER 4

BIPOLAR IMPLEMENTATION OF NON LINEAR FUNCTIONS

4.1 INTRODUCTION

In the previous chapter we have analyzed and generated various terms in current mode which are used in this chapter for generation of trigonometric functions, exponential functions, logarithmic function, sigmoid and Gaussian function. The realization of these functions is done with Taylor Series Approximation method. These functions are simulated in PSPICE A/D and their behavior is compared with their ideal behavior by collecting data points from PSPICE A/D and tracing in MATLAB along with ideal functional graph.

4.2 TAYLOR SERIES EXPANSION

It states that any function f(x) can be expressed as below:

$$f(x) = \sum_{K=0}^{\infty} p_K (X - X_0)^K \tag{4.1}$$

Where,

$$p_K = \frac{1}{K!} f^{(K)}(X_0) \tag{4.2}$$

The above equations 4.1 and 4.2 will be helpful while approximating the functions as explained below in this chapter.

4.3 GENERATION OF GAUSSIAN FUNCTION

Gaussian function can be expressed mathematical [2] as shown in equation below, and can also be approximated with the help of Taylor series expansion as:

$$f(h) = e^{-h^2} \tag{4.3}$$

$$f(h) = e^{-h^2} \cong 1 - h^2 + \frac{h^4}{2} \qquad |h| \leq 1 \tag{4.4}$$

This function can be generated using the above proposed modules in chapter 3 as shown below in Fig 4.1

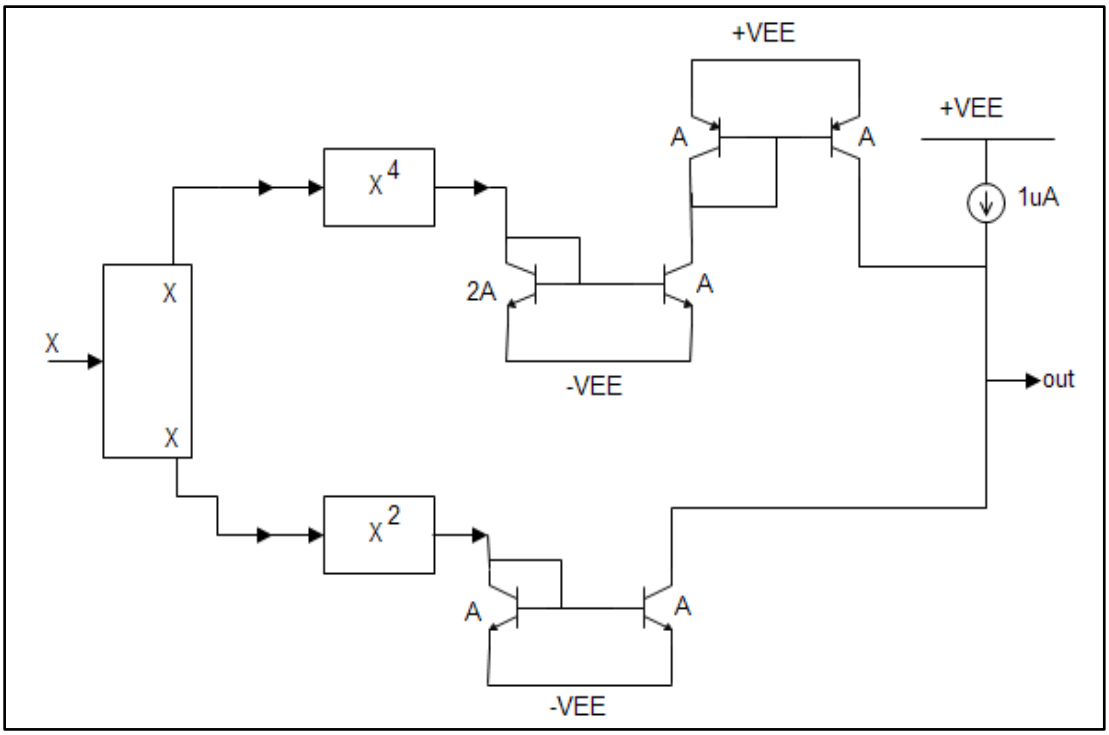

Fig 4.1 Gaussian Block

4.3.1 DC TRANSFER CHARACTERISTICS OF GAUSSIAN BLOCK

The DC transfer characteristics of this function is simulated in PSPICE A/D using bipolar transistors NR200N and PR200N of ALA400 from AT&T Company for input current signal varying from -1uA to +1uA, keeping power supply equal to ±3.65V. The DC characteristic is shown as below in Fig 4.2.

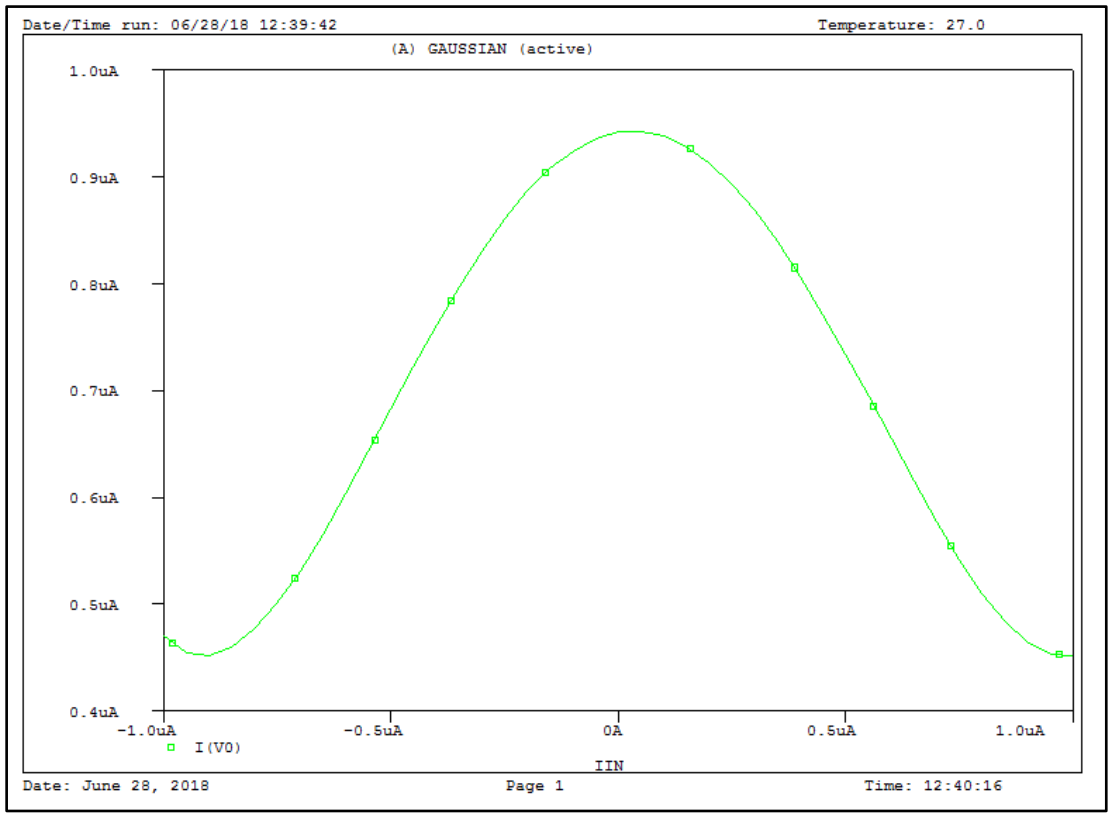

Fig 4.2 Gaussian Function Plot

4.3.2 COMPARISON WITH IDEAL CHARACTERISTIC

Our circuit has close proximity to the ideal graph of this function as shown in Fig 4.3 below. Blue color graph shows the simulated results and red color graph shows the ideal results. These graphs are traced in MATLAB.

The percentage error for this realized circuit is shown in Fig 4.4 with maximum percentage of error value reaching to 13.8% at input current value of 0.68uA, and minimum percentage of error value equal to 1% at input current value of 0.8uA. This graph is also traced in MATLAB.

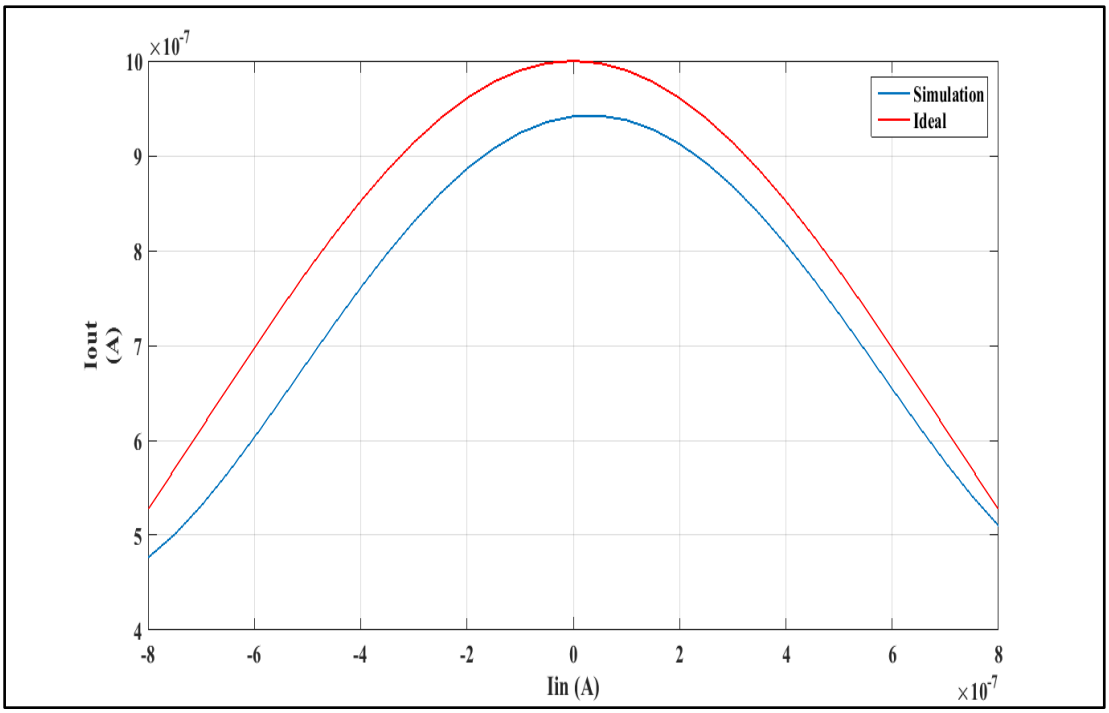

Fig 4.3 Comparison graph with Ideal Characteristics

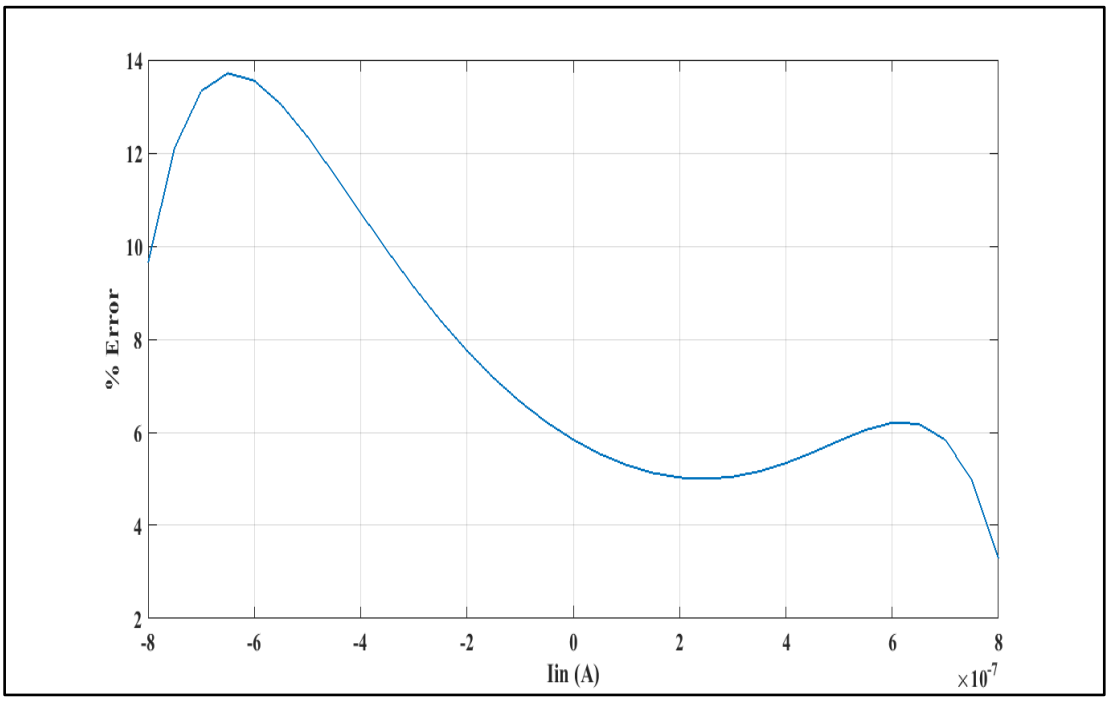

Fig 4.4 Percentage error graph

4.3.3 APPLICATION OF GAUSSIAN FUNCTION

As studied from reference [2], [3], this function has major application in artificial neural networks while generating activation function. Since this circuit is in current mode thus provide us with better range and faster response.

4.4 GENERATION OF SIGMOID FUNCTION

Sigmoid function is S shaped function [4], with mathematical representation as:

$$f(h) = \frac{1}{1+e^{-h}} \tag{4.5}$$

Its approximation to the order of three with the help of Taylor series expansion is written as

$$f(h) \cong \frac{1}{2} + \frac{h}{4} - \frac{h^3}{48} \tag{4.6}$$

This function can be generated by using the above block is shown in fig 4.5 below.

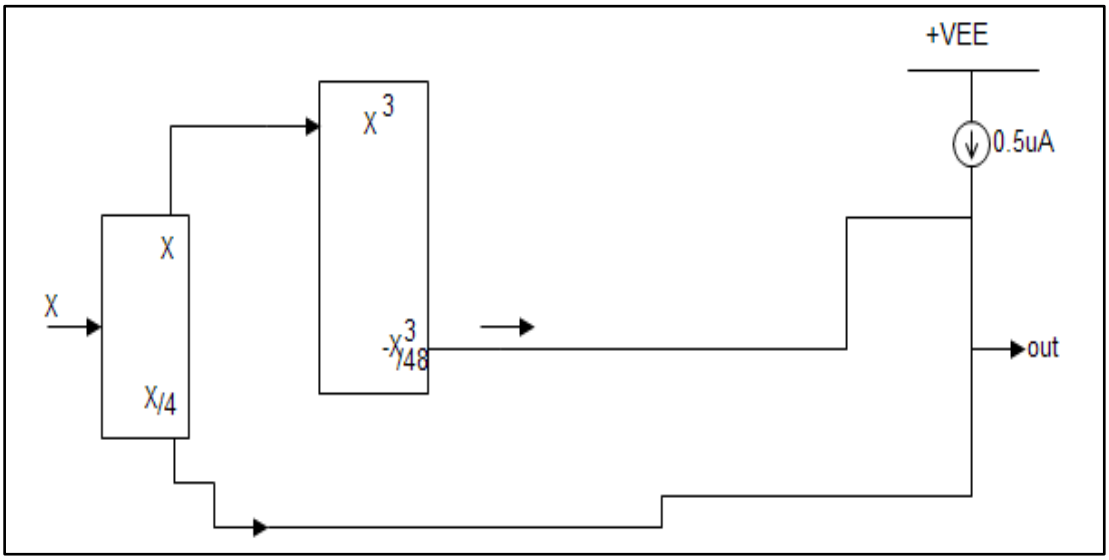

Fig 4.5 Sigmoid Block

4.4.1 DC TRANSFER CHARACTERISTIC OF SIGMOID BLOCK

The DC transfer characteristic of this function is shown in Fig 4.6 which is simulated in PSPICE A/D for input current signal varying from -1.5uA to +1.5uA and keeping power supply equal to ±3.65V.

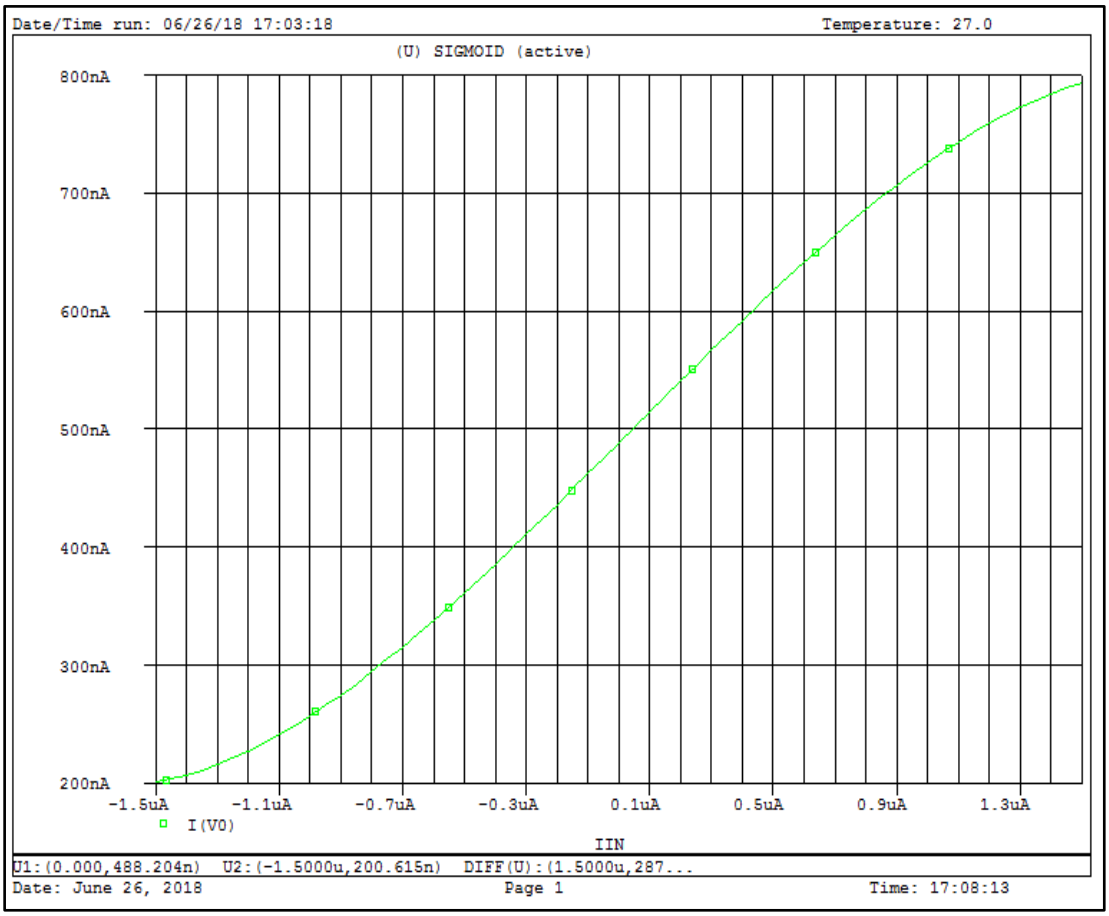

Fig 4.6 DC characteristics of Sigmoid Block

4.4.2 COMPARISION WITH IDEAL CHARACTERISTICS

The Fig below 4.7 shows the comparison graph with the ideal characteristics consisting of blue plot showing the simulated result and red plot showing the ideal result. This plot is traced in MATLAB and our approximated function shows the results which are closely equal to the ideal characteristics with some amount of error which can be observed in Fig 4.8.

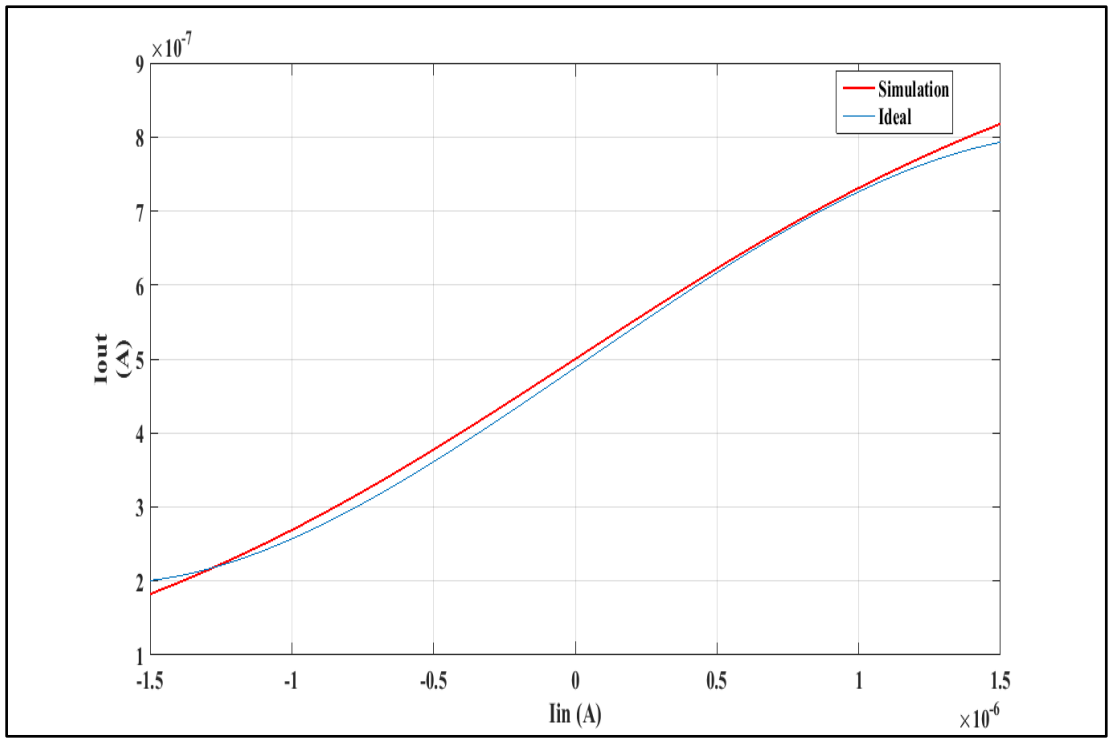

Fig 4.7 Sigmoid comparison graph with ideal characteristics

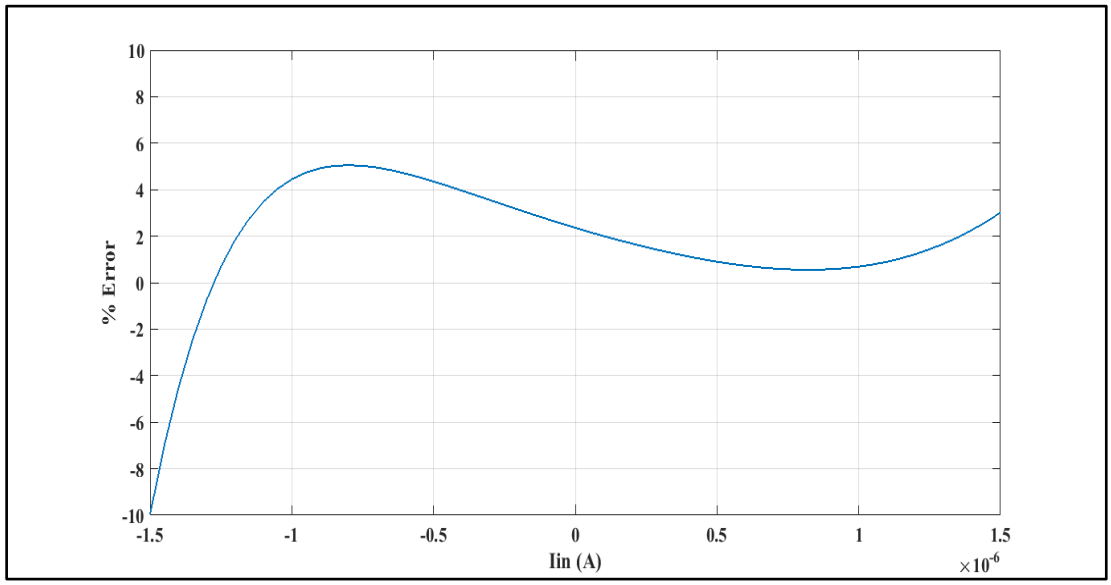

Fig 4.8 Percentage Error Graph for sigmoid function

From the Fig 4.8 shown above it is observed that the magnitude of the maximum percentage of error for sigmoid function with ideal value is 10% at the

input current value of 1.5uA and minimum percentage of error is 0.5% at the input current value of 0.75uA.

4.4.3 APPLICATION OF SIGMOID FUNCTION

The major application of this block is in artificial neural network where activation functions are used as sigmoid function [4]. This block is a bipolar implementation hence provides us faster response.

4.5 GENERATION OF TANGENT HYPERBOLIC INVERSE FUNCTION

Tangent hyperbolic inverse function [5] can be mathematically represented as:

$$tanh^{-1}(u) = \frac{1}{2}\ln\left(\frac{1+u}{1-u}\right) \tag{4.7}$$

This can be approximated to order of five with Taylor series expansion as follows:

$$f(u) \cong u + \frac{u^3}{3} + \frac{u^5}{5} \tag{4.8}$$

The above approximated function can be implemented using the basic modules derived in chapter 3 as shown in Fig 4.9 below. The scaling of fifth order term for implementation of this function can be done with the help of inverting current mirror configuration as shown in Fig 4.9.

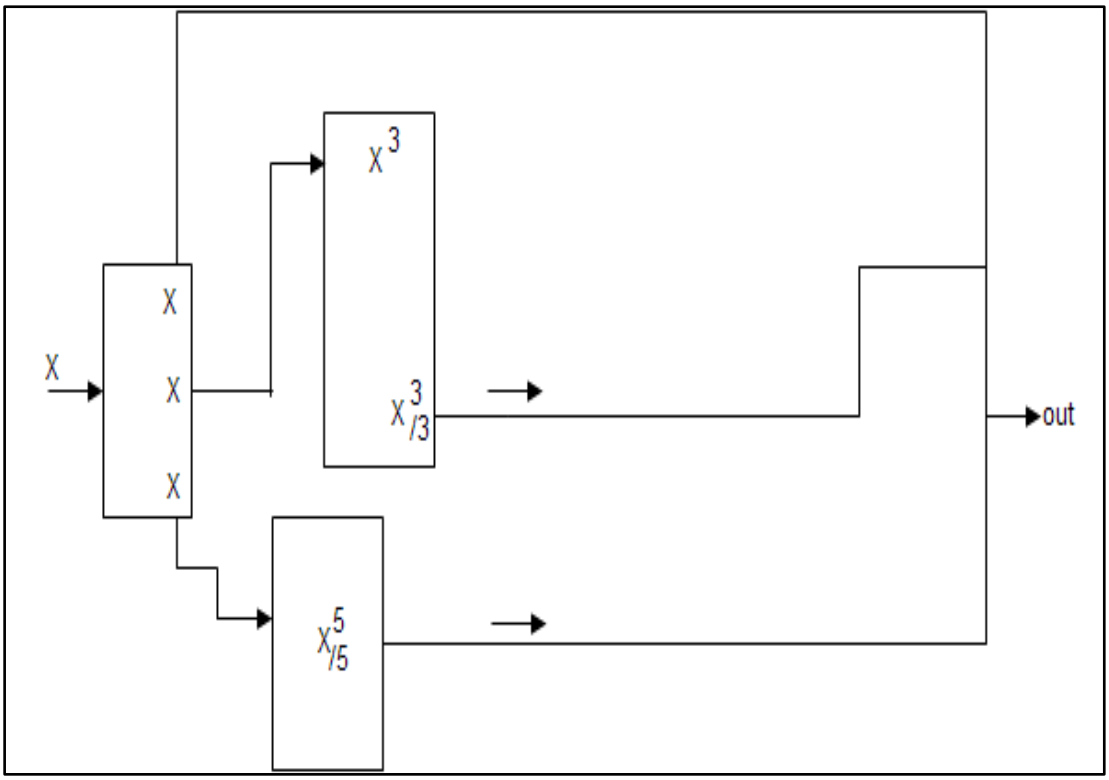

Fig 4.9 Tangent Hyperbolic Inverse Block

The scaled term of third order term is used from the cubic that is generated in cubic block in chapter 3. Also the number of linear outputs can be increased with the help of current mirror in the linear circuitry shown in chapter 3.

4.5.1 DC TRANSFER CHARACTERISTICS OF TANGENT HYPERBOLIC INVERSE FUNCTION

A DC transfer characteristic of Tangent hyperbolic inverse function is analyzed in PSPICE A/D for input current varying from -1uA to +1uA and keeping the power supply equal to ±3.65V. The DC transfer characteristic is shown in Fig 4.10 below.

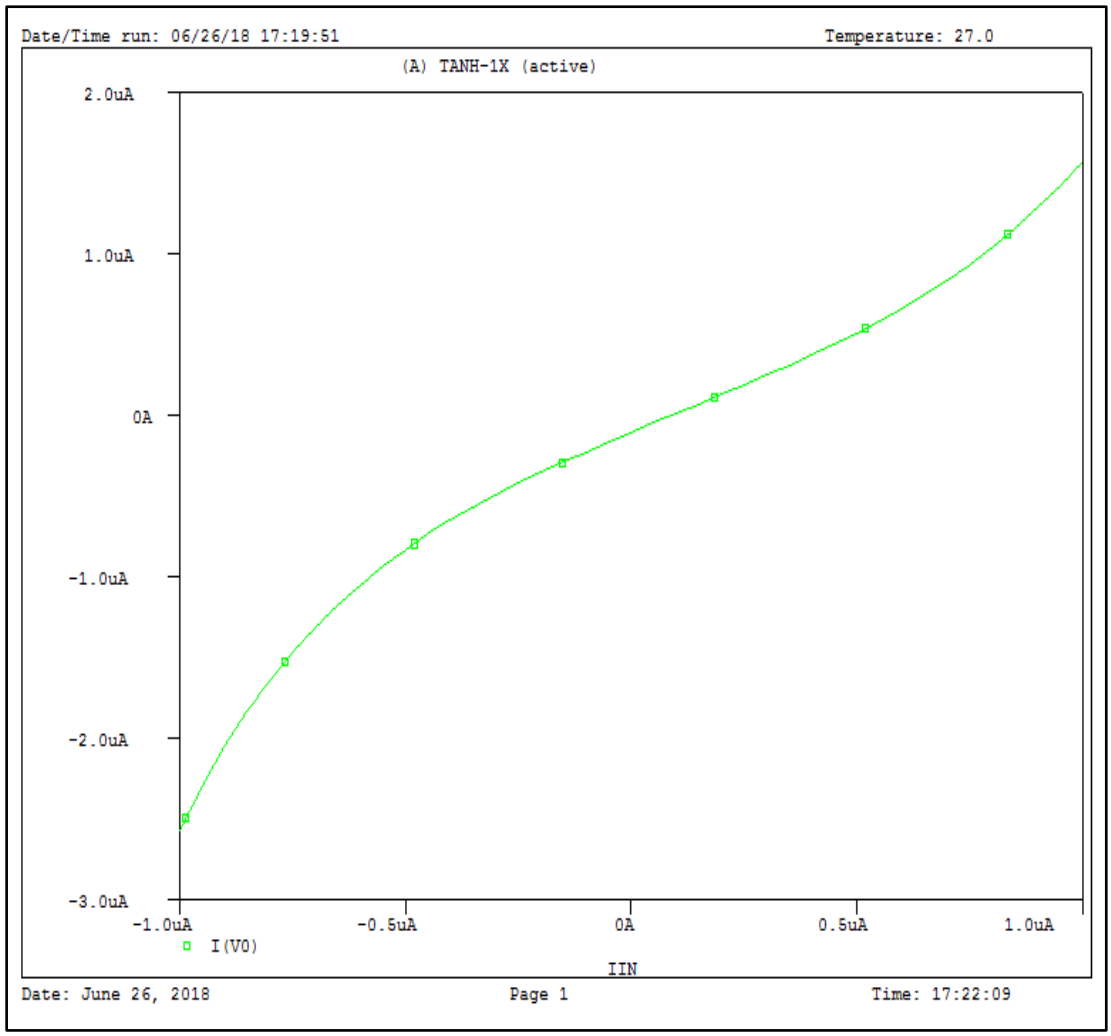

Fig 4.10 Tangent Hyperbolic Inverse Function Plot

4.5.2 COMPARISON OF TANGENT HYPERBOLIC INVERSE FUNCTION WITH ITS IDEAL CHARACTERISTIC

The plot for comparison with the ideal characteristics of this function is shown in Fig 4.11 below which is plotted in MATLAB consisting of blue color plot representing the simulated result and red plot representing the ideal result. The error graph is shown in Fig 4.12 below.

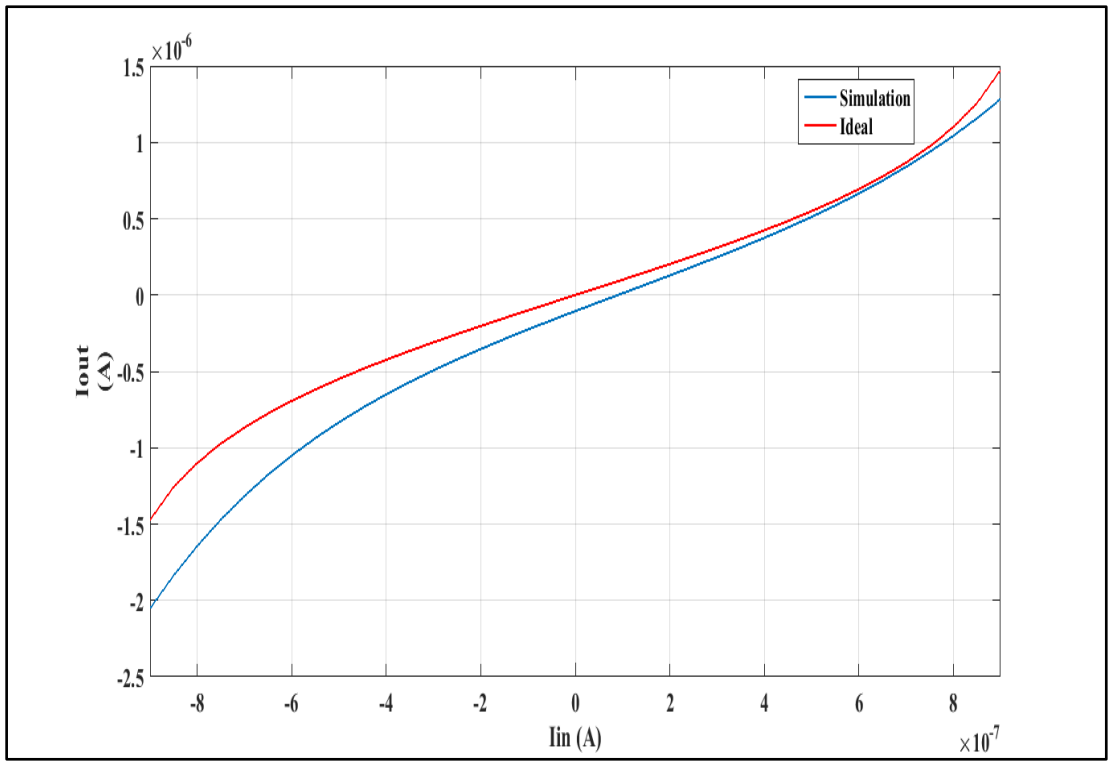

Fig 4.11 Comparison Graph with Ideal Characteristics

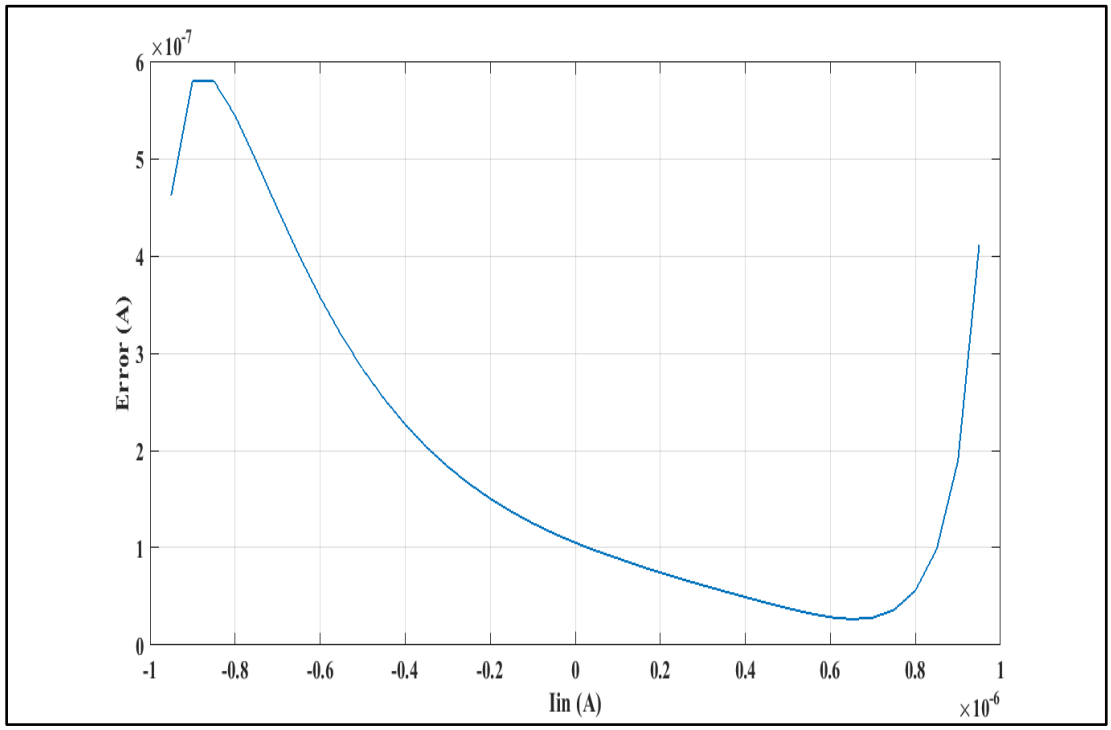

Fig 4.12 Error graph for tangent hyperbolic function

It is easily observable from the above Fig 4.12 that maximum error is of 0.58uA at the input value of 0.9uA and minimum error value of .02uA at input current value of 0.7uA.

4.6 GENERATION OF EXPONENTIAL FUNCTION

The exponential function [1] mathematically represented as equation shown below:

$$f(h) = e^h \tag{4.9}$$

This can be approximated with the help of Taylor series expansion as follows:

$$f(h) = e^h \approx 1 + h + \frac{h^2}{2} + \frac{h^3}{6} + \frac{h^4}{24} \tag{4.10}$$

The implementation of this function is done by using linear block, square block, cubic block and fourth order block that has been proposed in chapter 3. The exponential implementation is shown in Fig 4.13 below.

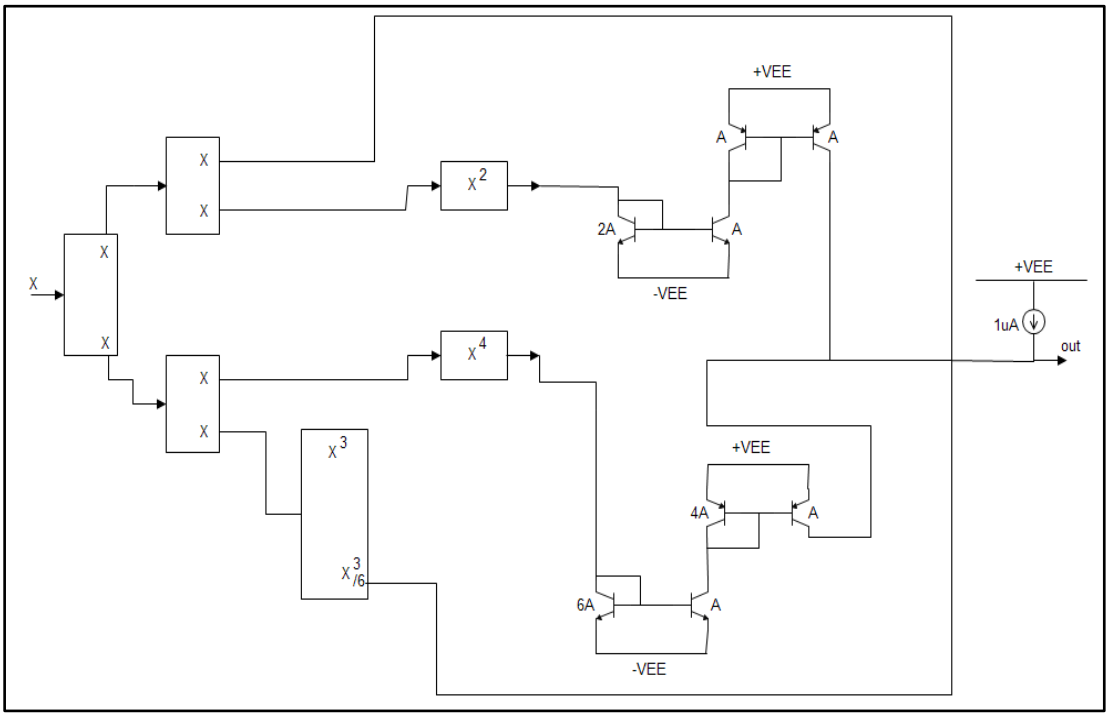

Fig 4.13 Exponential Block

It should be noted here that for scaling of square term we have used an non inverting current mirror in order to generate positive scaled square tem, also with area twice that of copier npn bipolar transistor, similarly for scaled fourth order term we have used non inverting current mirror along with area six times of first transistor than of second in npn current copier circuit and four times of third transistor with respect to fourth transistor in order to generate scaling factor of 24.

4.6.1 DC TRANSFER CHARACTERISTICS OF EXPONENTIAL BLOCK

The analysis of DC transfer characteristics is done in PSPICE A/D for varying input signal ranging from -0.6uA to +1.5uA and keeping power supply equal to ± 3.65V. The DC characteristic graph is shown in Fig 4.14 below.

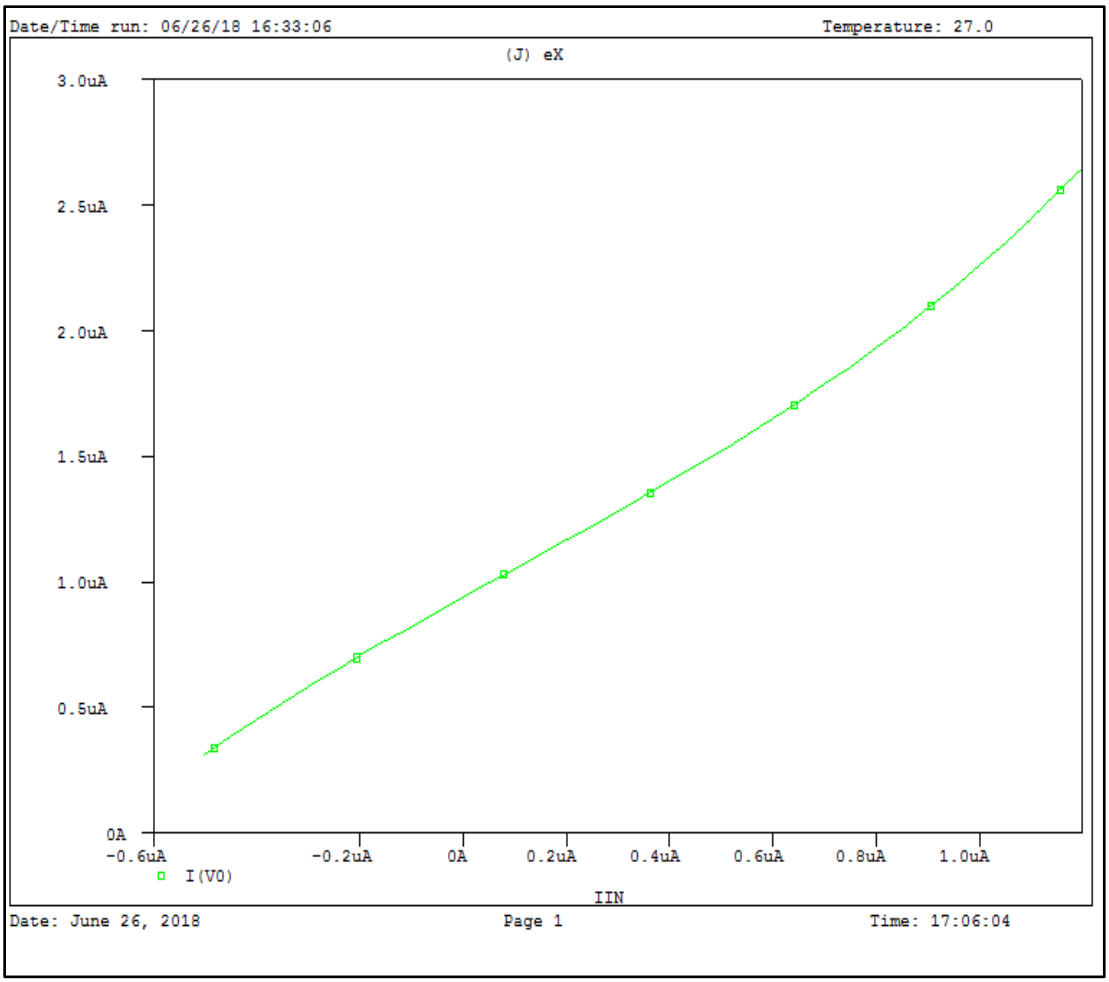

Fig 4.14 DC transfer characteristics of exponential block

4.6.2 COMPARISON WITH IDEAL CHARACTERISTIC FOR EXPONENTIAL FUNCTION

The comparison is done with ideal behavior of exponential function in MATLAB, where the plot has been traced between simulated and ideal results, the graph shown have a plot in blue and red color for simulated and ideal characteristics respectively shown in Fig 4.15 below. The percentage error graph is also shown in Fig 4.16 below.

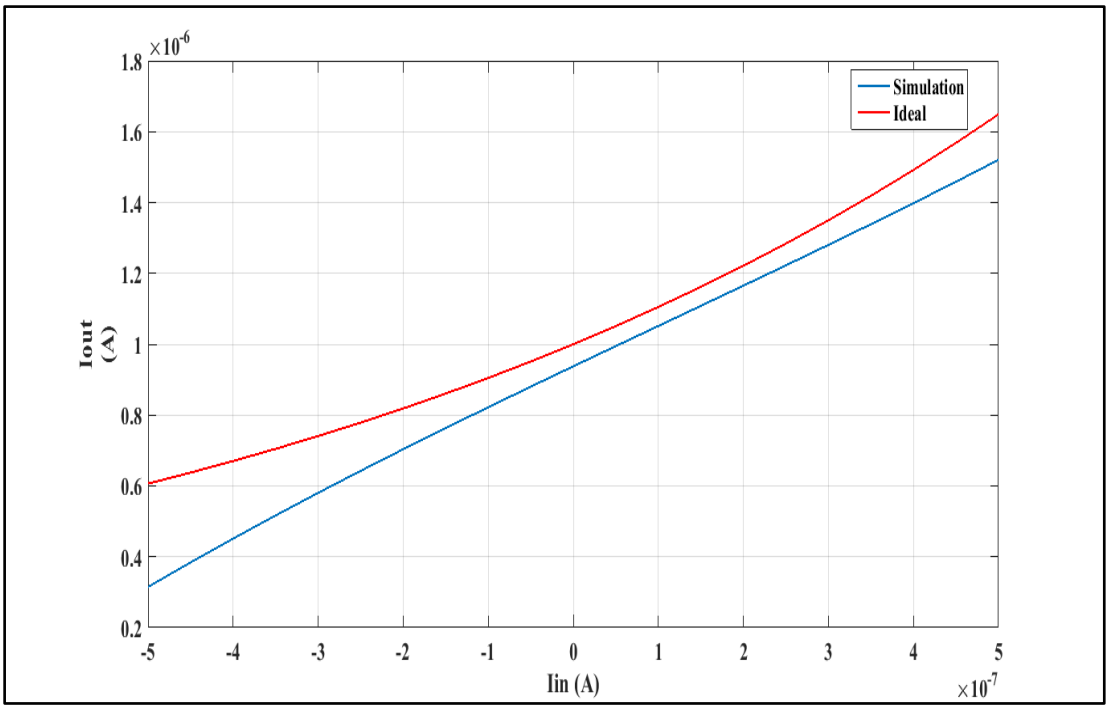

Fig 4.15 Comparison graph for exponential function

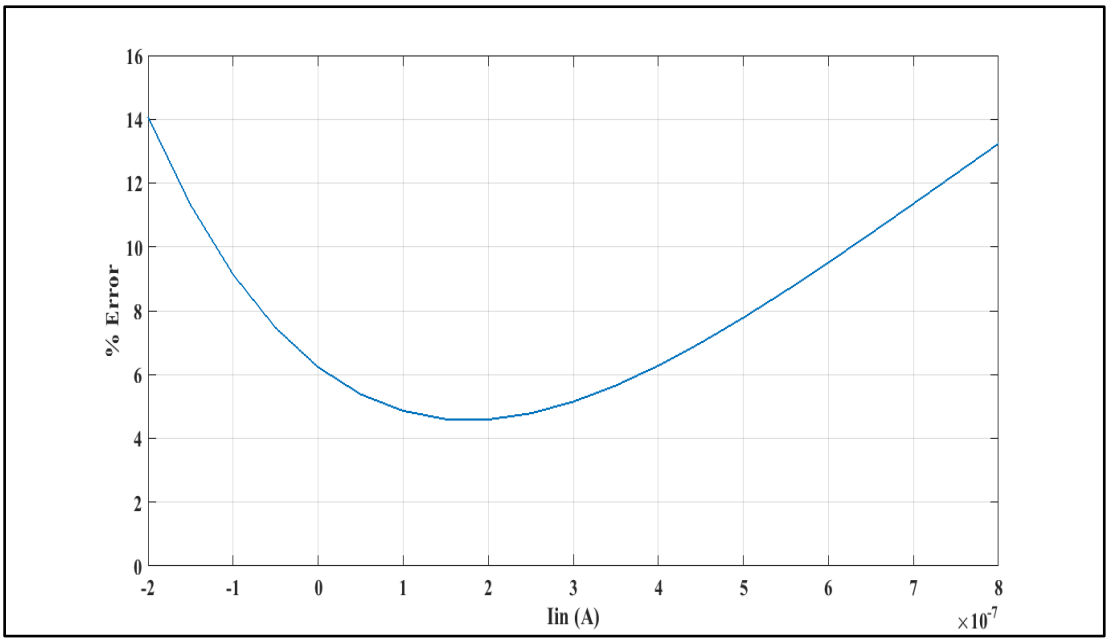

Fig 4.16 Percentage error graph for exponential function

It is observable that maximum percentage error is 14% at the input current value of -0.2uA because of offset at near zero, and minimum percentage error of 4.2% at input current +0.15uA. The error in this implementation is increased because of the increment of current more copier circuits used for scaling purpose.

4.7 GENERATION OF LOGARITHMIC FUNCTION

The Logarithmic function [1] can be mathematically expressed as below:

$$f(h) = \ln(1+h) \tag{4.11}$$

This can be approximated with Taylor series as below:

$$f(h) = \ln(1+h) \approx h - \frac{h^2}{2} + \frac{h^3}{3} - \frac{h^4}{4} \tag{4.12}$$

This approximated equation can be implemented using linear, scaled square, cubic and fourth order terms as shown in Fig 4.17 below. It should be noted from the Fig 4.17 that we have scaled the square and fourth order terms with the help of non inverting current mirrors, where scaling of square term can be done by

keeping the area of first npn bipolar transistor of npn current mirror equal to twice that of copier npn bipolar transistor in npn current mirror configuration also in order to scale fourth order term we have made the first npn bipolar transistor area equal to four times to the copier npn bipolar transistor in this current mirror configuration.

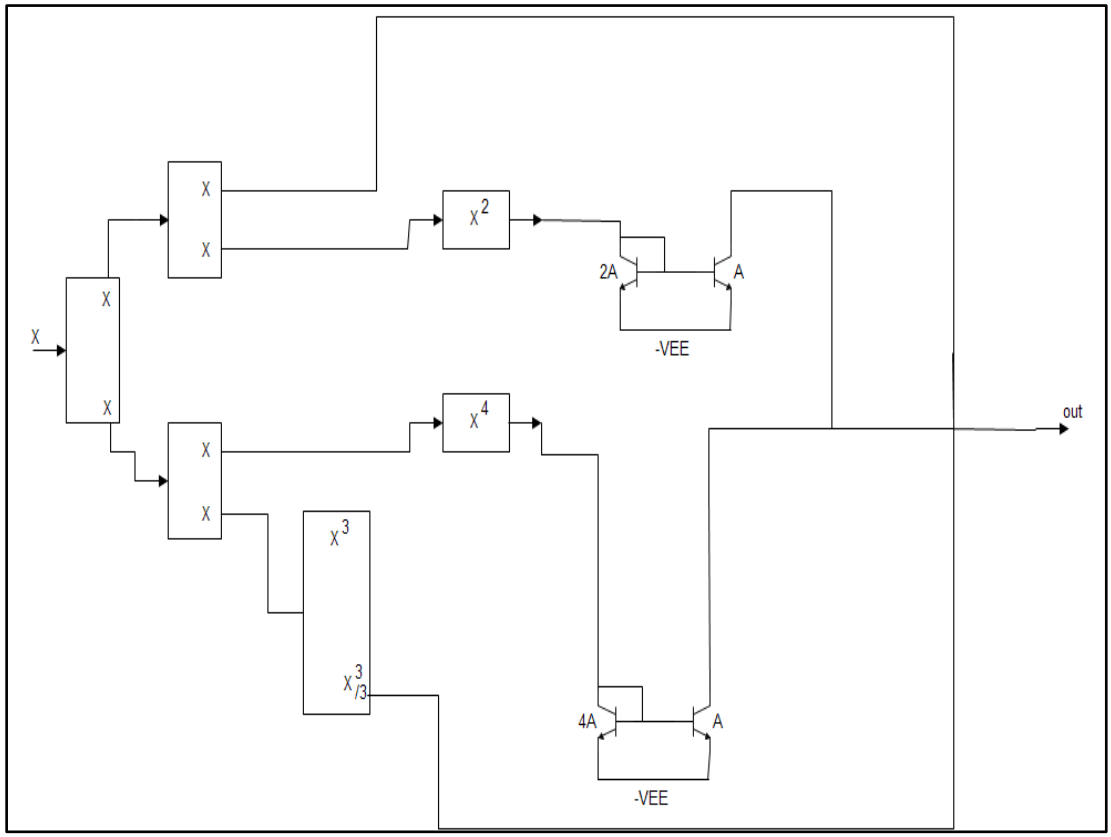

Fig 4.17 Logarithmic block

4.7.1 DC TRANSFER CHARACTERISTIC OF LOGARITHMIC BLOCK

The DC analysis of this block is done in PSPICE A/D by varying input current range from 0uA to +1uA. And keeping the power supply equal to ±3.65V. This analysis is shown in Fig. 4.18 below.

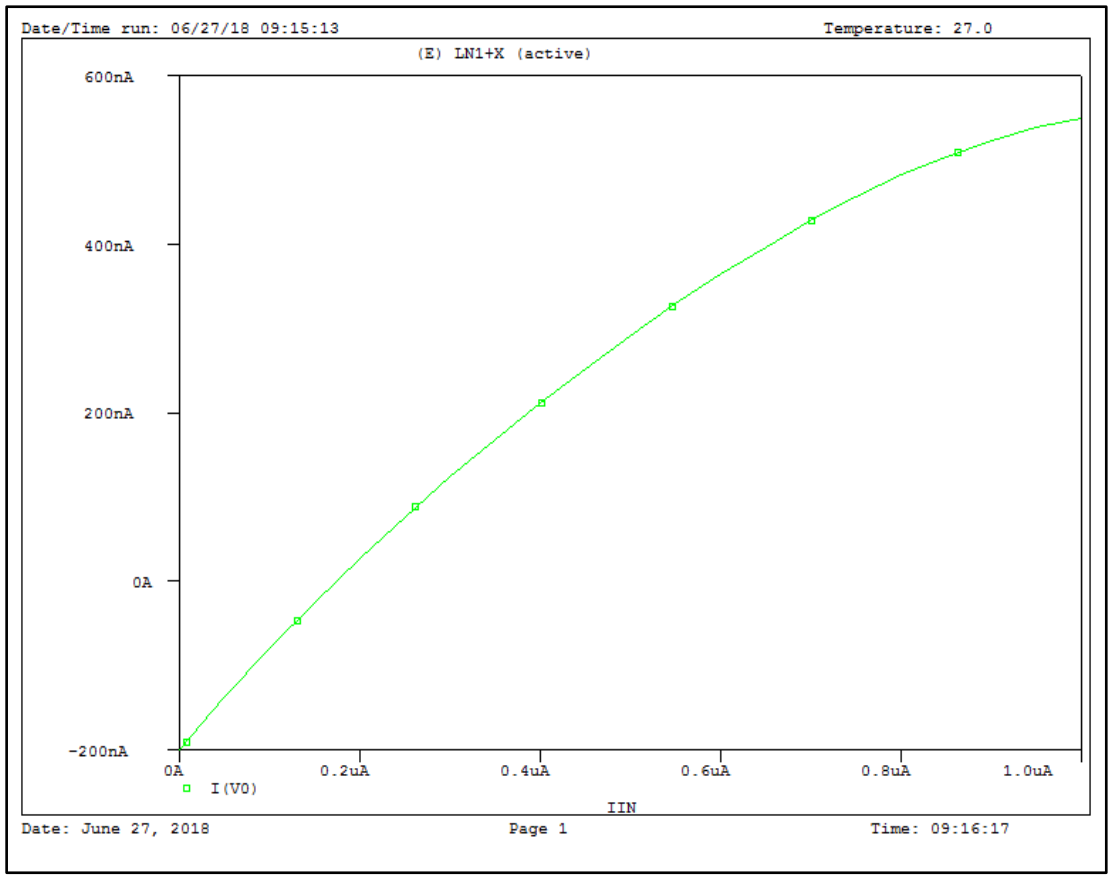

Fig 4.18 Logarithmic Block DC characteristic plot

4.7.2 COMPARISON WITH IDEAL LOGARITHMIC FUNCTION

The comparison with ideal logarithmic function is plotted in MATLAB as shown in fig 4.19 below, where blue color graph indicates the simulated result and red color graph shows the ideal result. The error graph is shown in Fig 4.20 and it is observed that the maximum offset is 0.2uA at input value of 0uA, and minimum offset is 0.1uA at input value of 0.7uA, which shows close behavior to ideal characteristics at small input current signal.

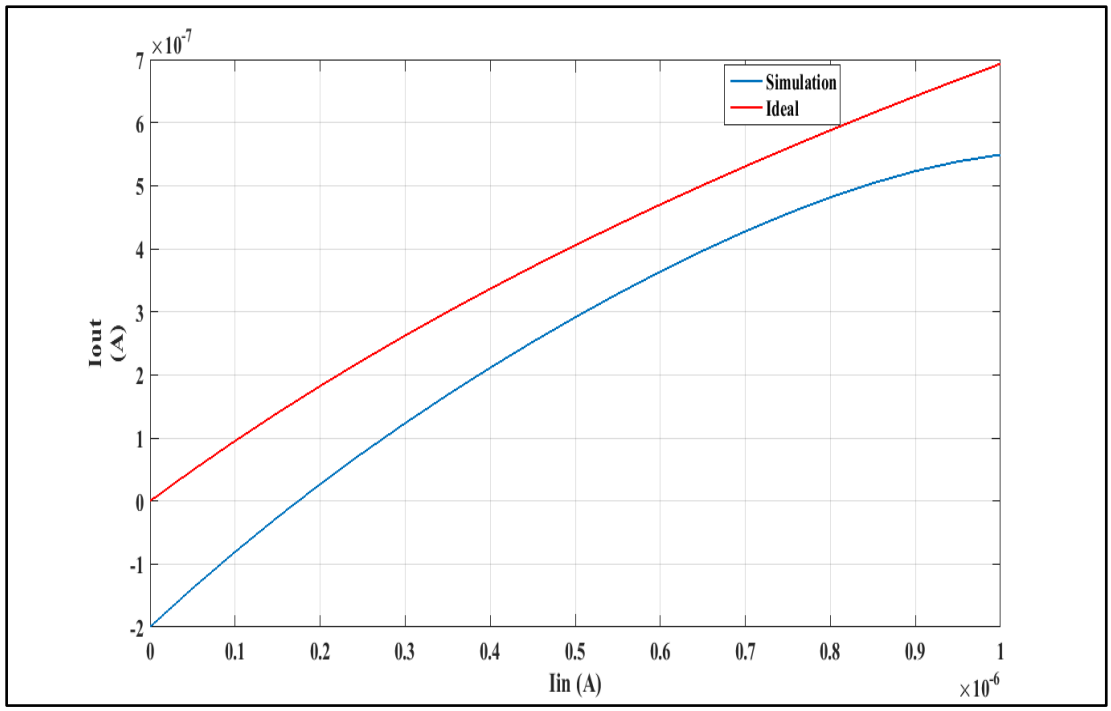

Fig 4.19 Comparison graph for logarithmic block

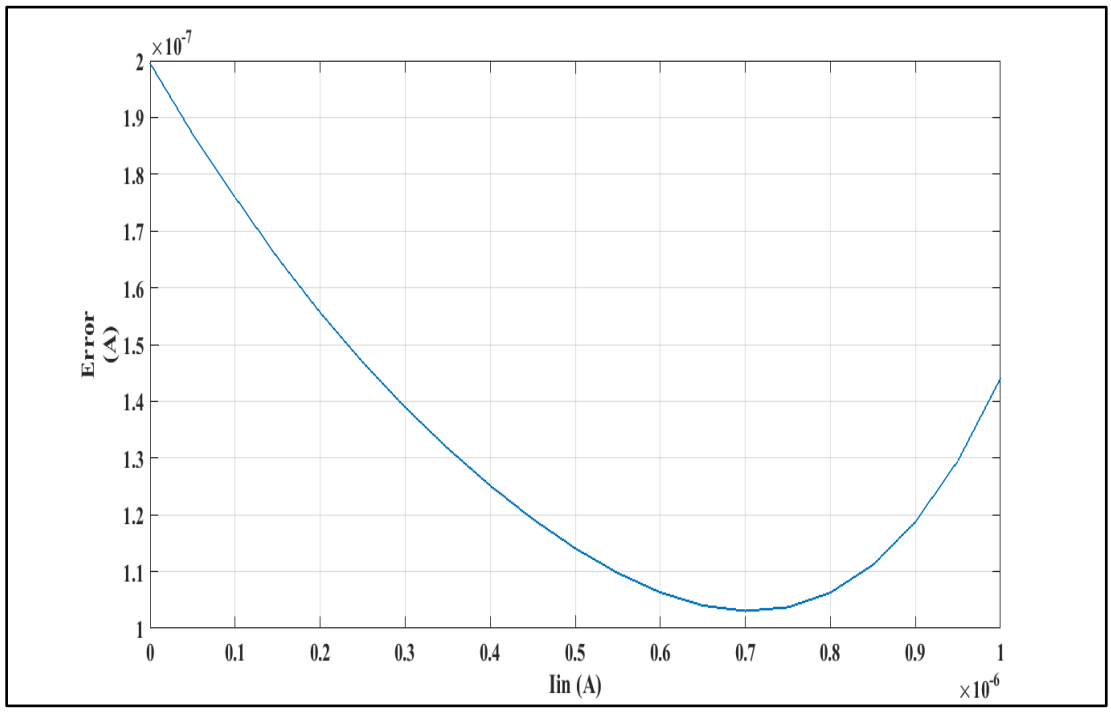

Fig 4.20 Error plot for Logarithmic block

4.8 GENERATION OF SINE FUNCTION USING BASIC MODULES

The Sine function is the one of the trigonometric function [6] which is approximated to third order using Taylor series expansion as given below:

$$f(h) = \sin(h) \cong h - \frac{h^3}{6} \tag{4.13}$$

This equation can be implemented using basic modules as shown in Fig 4.21 below using only blocks i.e. linear and cubic blocks.

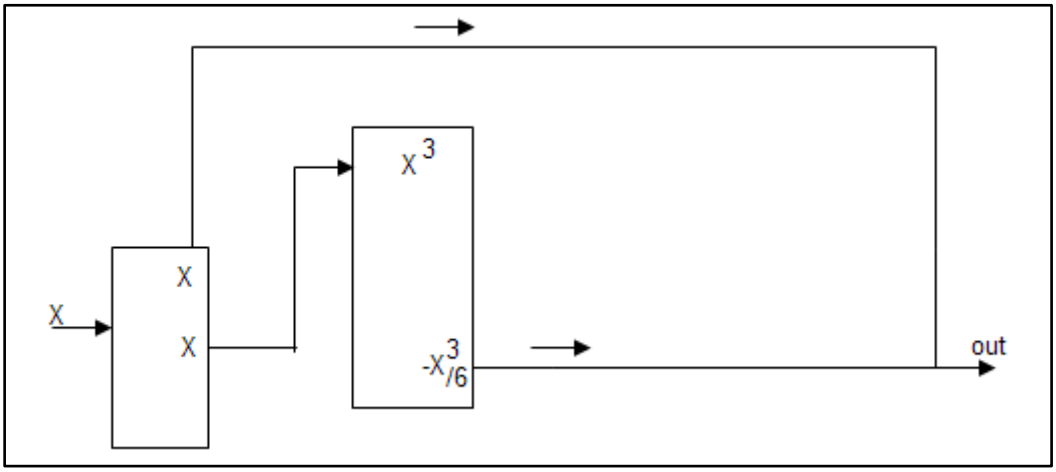

Fig 4.21 Sine Function Generator Block

4.8.1 SINE FUNCTION DC ANALYSIS

The DC analysis of this block or function is simulated in PSPICE A/D for the input current ranging from -1uA to +1uA as shown in Fig 4.22 below.

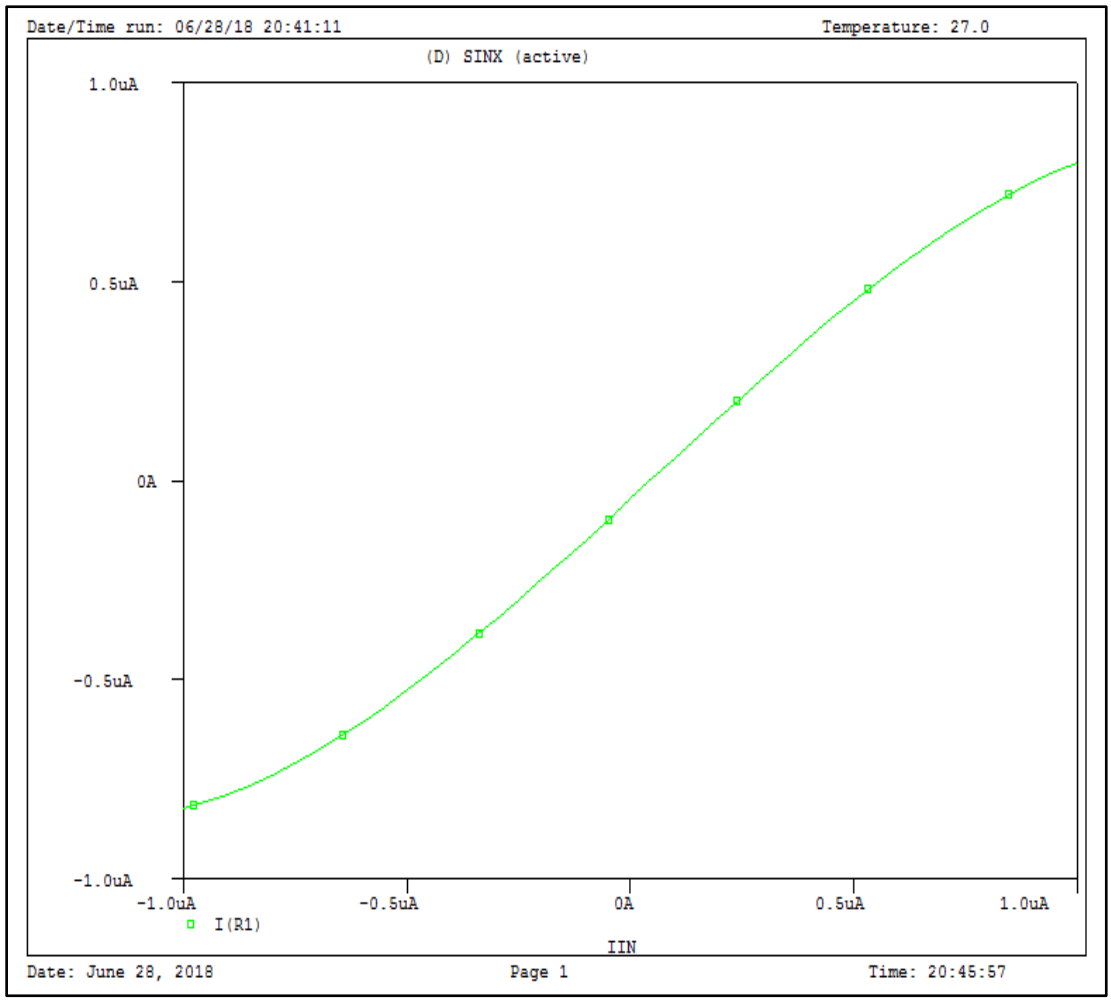

Fig 4.22 Sine function plot

4.8.2 COMPARISON WITH IDEAL CHARACTERSTIC FOR SINE FUNCTION

This behavior of the sine function in Fig 4.22 is compared with ideal characteristic as shown in Fig 4.23, where we presented the simulated result in blue color and ideal result in red color. The error plot for this function is shown in Fig 4.24 below where y-axis represents the error values and x-axis represents the input current values ranging from -1uA to +1uA.

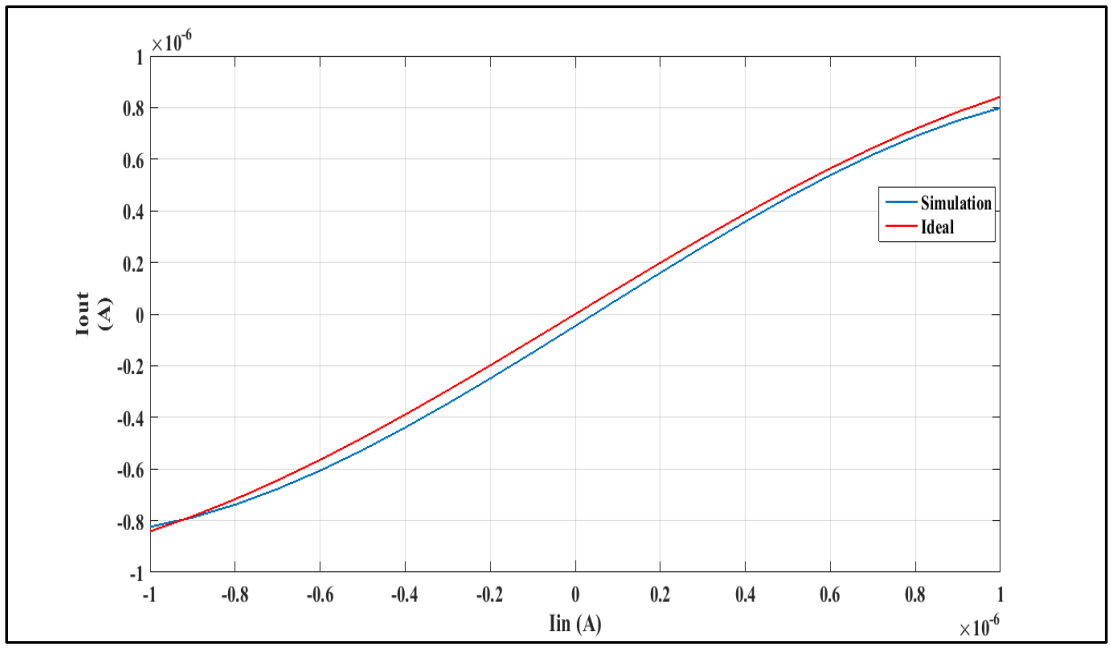

Fig 4.23 Comparison Plot for Sine Function

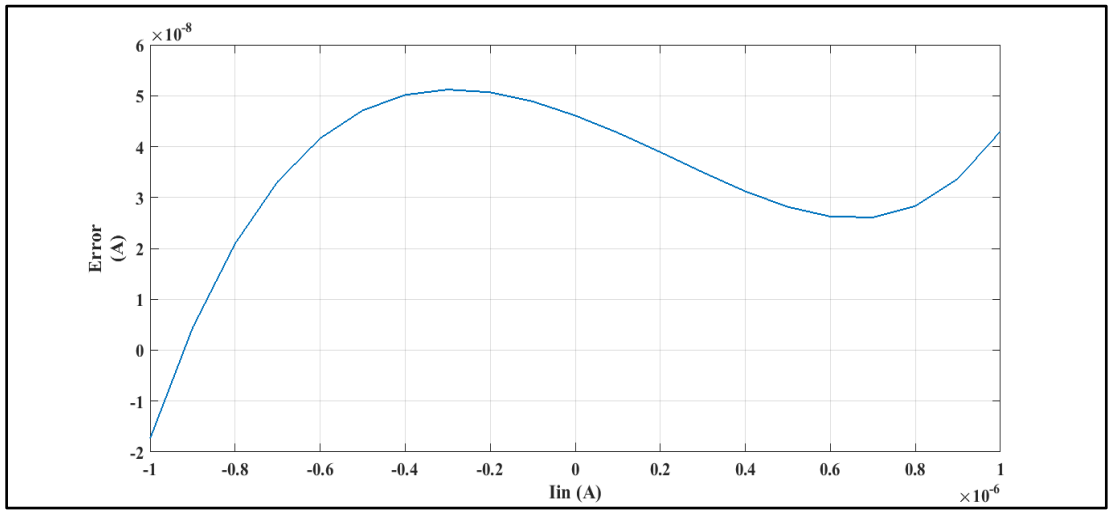

Fig 4.24 Error graph for Sine Function

From the error plot it can be observed that maximum deviation is of 0.05uA at input current of -0.38uA and the closest result is 0uA at input current value of -0.92uA.

4.9 GENERATION OF COSINE FUNCTION

This trigonometric function [1], [6] is approximated by Taylor series expansion to the order of four as expressed below.

$$f(h) = \cos(h) \cong 1 - \frac{h^2}{2} + \frac{h^4}{24} \tag{4.14}$$

This approximated equation can be implemented with the help of squarer and power four blocks as shown in Fig 4.25 below.

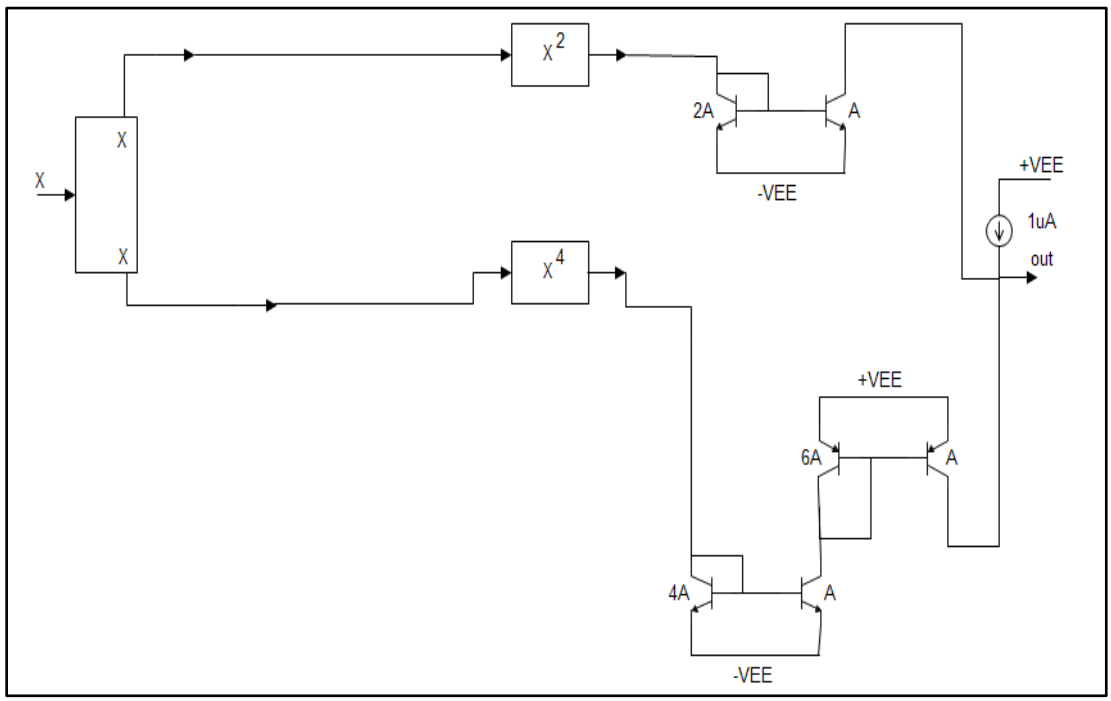

Fig 4.25 Cosine block

The block shown above have inverting and non inverting current mirror configuration to generate the scaled terms.

4.9.1 DC TRANSFER CHARACTERISTICS OF COSINE BLOCK

The DC characteristics of this block is simulated in PSPICE A/D using same transistor models for current mirror configuration which are NR200N and PR200N, with power supply for the circuit equal at ±3.65V, the output is observed for the input range of -1uA to +1uA as shown in Fig 4.26 below.

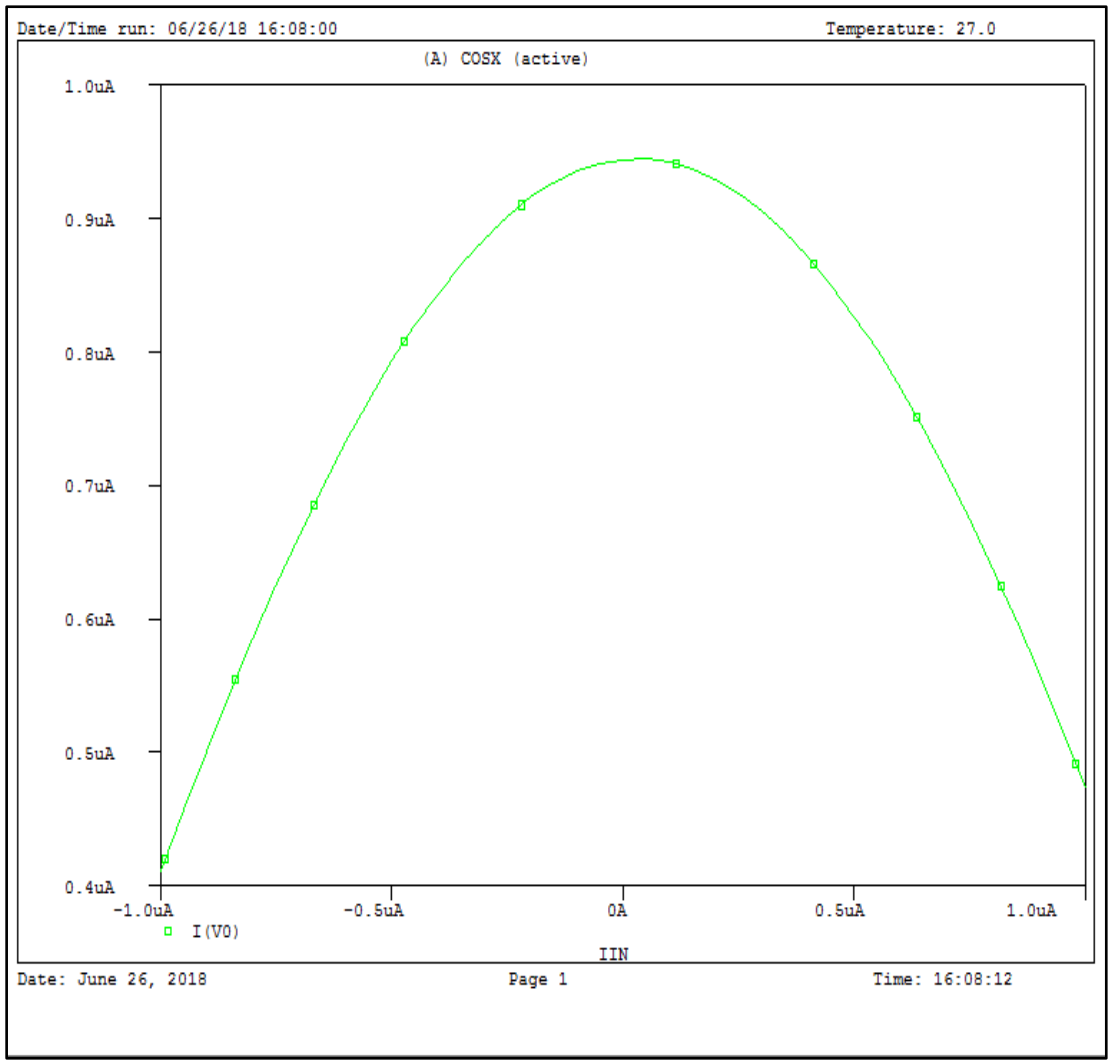

Fig 4.26 Cosine DC transfer characteristics

4.9.2 COMPARISON OF IMPLEMENTED BLOCK WITH IDEAL COSINE FUNCTION

The comparison is done in MATLAB by plotting the function's simulated and ideal results in blue and red color graph respectively as shown in Fig 4.27 below.

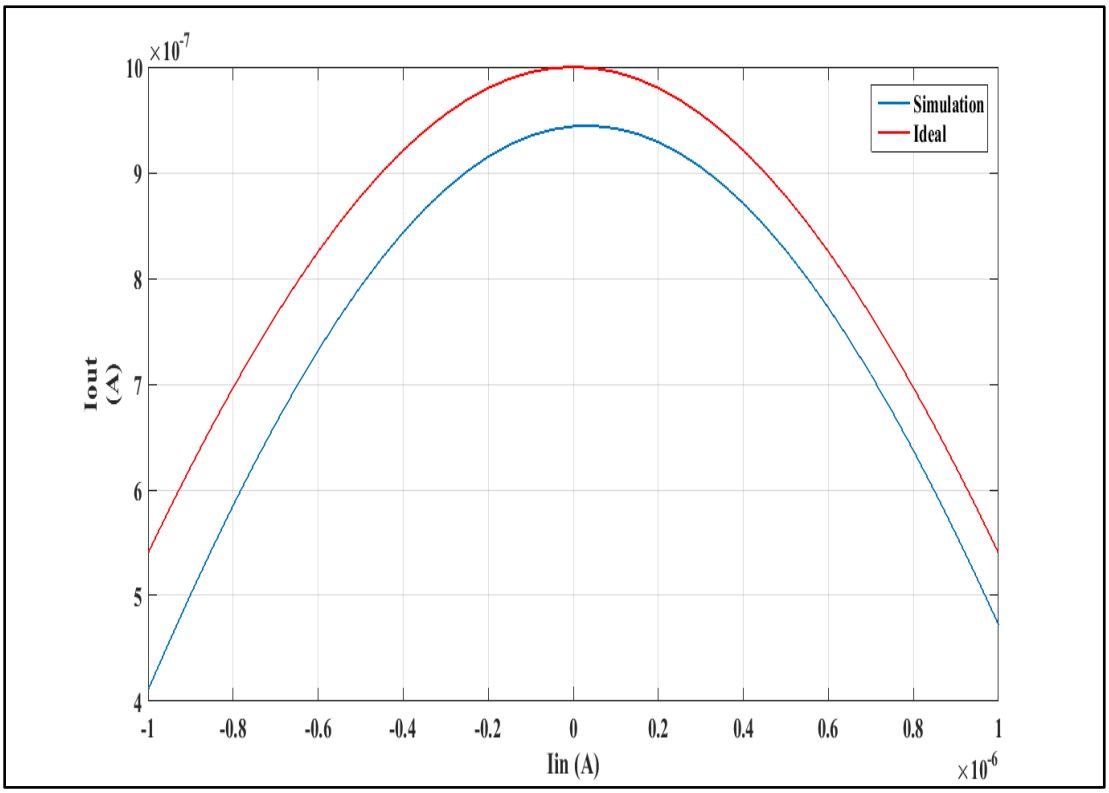

Fig 4.27 Comparison Graph for Cosine function

The Fig 4.28 below shows the percentage error graph for this function which decreases as we move towards the origin and reaches to a minimum difference of 5% for input current value of 0.2uA. This difference is maximized at input current of value -0.8uA which is equal to 16%.

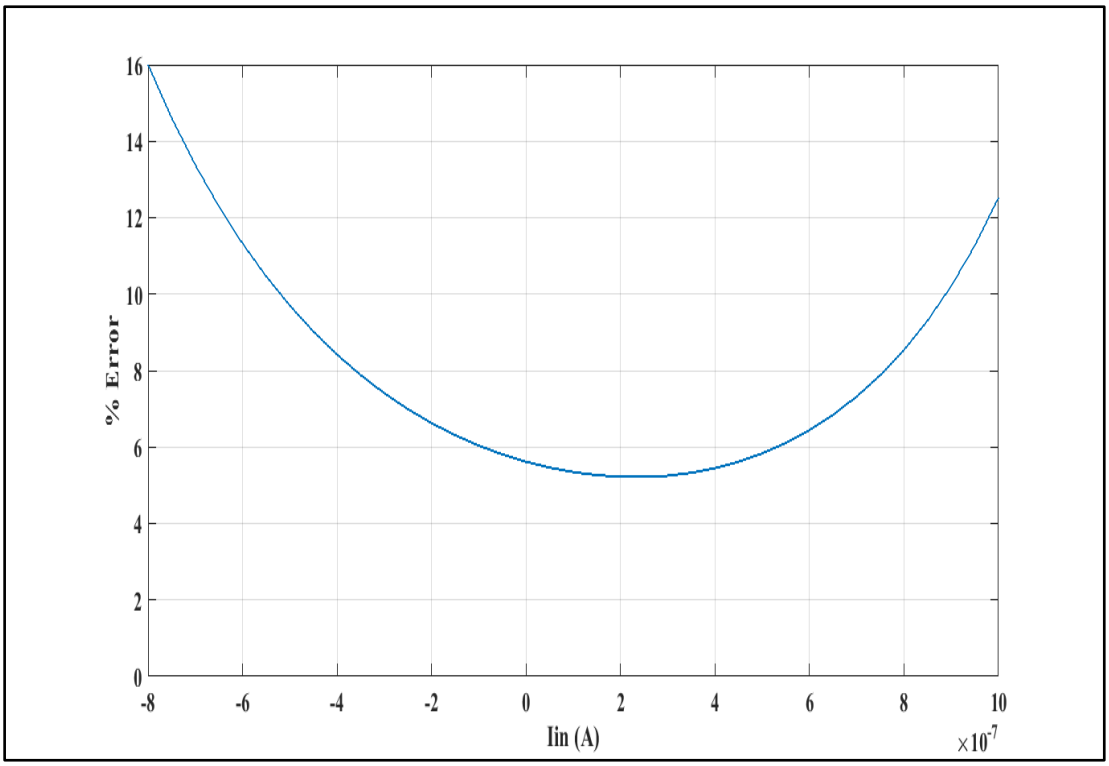

Fig 4.28 Percentage error graph for Cosine function

4.10 CONCLUSION

In this chapter we have implemented various functions which have many applications in the field of non linear analog signal processing as needed in artificial neural network for generation of activation functions. It should be noted that as the number of transistors increases in a circuitry the deviation from the desired values increases, hence approximated functions which have terms up to fourth order gives good results i.e. having less percentage of error as compared to those functions which are approximated up to fifth order. The above functions realized can be made closer to ideal values by introducing the offset circuitry along with those circuits.

REFRENCES

[1] E. Kreyszig, Advanced Engineering Mathematics, eds.8,Wiley Publications,9-788126-508273.

[2] M.T. Abuelma'atti, S.R. Al-Abbas, "A New Analog Implementation for the Gaussian Function," *IEEE Indutrial Electronics and Application Conference*, 2016,pp.216-224,978-1-5090-0925-1/16.

[3] T. M. Khaneshan, M. Nematzadeh, A. Khoei, K. Hadidi, "An Analog Reconfigurable Gaussian-Shapped Membership function Generator using Current-Mode techniques," *IEEE Iranian Conference on Electrical Engineering*,2012,978-1-4673-1148-9/12.

[4] Khodabandehloo G., Mirhassani M., Ahmadi M., "Analog Implementation of a Novel Resistive-Type Sigmoidal Neuron," *IEEE trans. On VLSI sytems*, vol.20,No.4,2012.

[5] Namin A.H., Leboeuf K., Muscedere R., Wu H., Ahmadi M., "Efficient hardware implementation of the hyperbolic tangent sigmoid function," *Proc. IEEE Int. Symp. Circuits Syst*., 2009, pp. 2117-2120.

[6] B. Gilbert, "A Monolithic Microsystem for Analog Synthesis of Trigonometric Functions and their Inverses," *IEEE J. Solid State Circuits*, SC-17,1179-1191,1982.

[7] M.H. Rashid, Introduction to PSpice Using OrCAD for Circuits and Electronics,eds.III,Pearson,2004.

CHAPTER 5

BIPOLAR IMPLEMENTATION OF ELLIPTIC CURVE FOR CRYPTOGRAPHY

5.1 INTRODUCTION

Security of systems is the major issue in today's life hence enhancement in security is to be updated from time to time. In field of information security, the systems on which security related work is prime focus are known as Cryptosystems [1], [2]. In these systems encryption and decryption techniques are implemented in order to make systems more secure. The each user is provided with a private key, with the help of this private key the intended user can only access to the given information. This private key plays the vital role for the security of information and one of the techniques to generate this private key is with the help of elliptic curve properties in digital systems. In this chapter we are going to implement this elliptic curve as one of the analog signal processing applications with the help of non linear blocks studied in previous chapters.

5.2 ELLIPTIC CURVE

This is the curve which is used for enhancement of security of our cryptosystems [1] shown in Fig 5.1 below. Before going to the digital implementation technique of this curve's properties we need to understand the basic equation of elliptic curve and some basic properties of this curve as mentioned below in this section.

Equation of elliptic curve is mathematically represented as:

$$y^2 = x^3 + ax + b \tag{5.1}$$

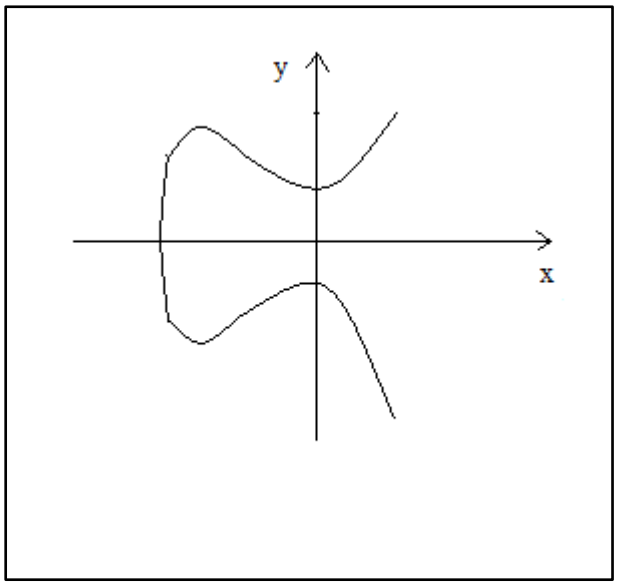

Fig 5.1 Elliptic Curve

5.2.1 PROPERTIES OF ELLIPTIC CURVE

There are two properties of this curve which is used for digital implementation of this curve which are as follows:

1) POINT DOUBLING:

Geometrically this property says that draw a tangent at a point and mark the other point which has the intersection between the curve and tangent, taking the mirror image of the intersected point with respect to x axis gives us the second point which is double to that of first point from where the tangent is drawn [1]. This property is shown in Fig 5.2 below. Implementation of this property is useful when we are required to find out the second point with the help of given single point.

$$R = 2T \tag{5.2}$$

2) POINT ADDITION

When we have two points and we want to find out the third point this graph has the property that after drawing the cord between these two points and extending it to new point of intersection on the curve and taking the mirror image of the obtained intersected point with respect to x-axis provides us the third required point which is holding the property as [1] [2]:

$$R = S + T \tag{5.3}$$

Graphical representation of this property is also shown in Fig 5.2 below.

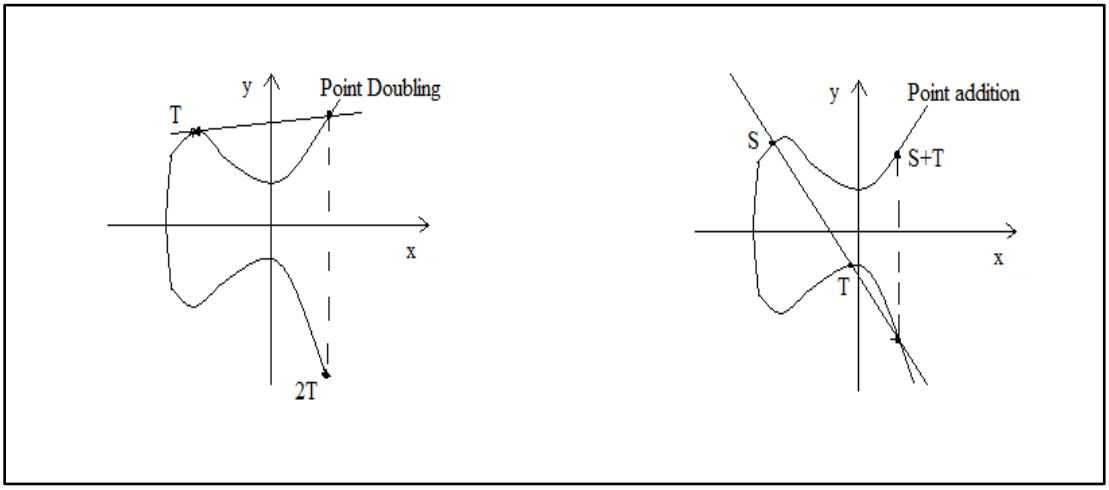

Fig 5.2 Properties Of Elliptic Curve

The points on the curve can be calculated with the help of above properties using the modulo p method [1]. Note that when there is case of finding mod p of any inverse value then we have to multiply that value whose inverse is taken with some number such that it gives the remainder equal to 1, and that number is result of modulo p. example: 2^{-1} mod 5 is 3, since multiplication of 2 with 3 gives us 6 and mod 5 of 6 is 1 hence result is 3.

$$x_3 = t^2 - x_1 - x_2 \, mod \, p \tag{5.4}$$

$$y_3 = t(x_1 - x_3) - y_1 \, mod \, p \tag{5.5}$$

Where,

$$t = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} mod \, p \, ; if \; T \neq S \; (point \; addition) \\ \frac{3x_1^2 + a}{2y_1} \, mod \, p \, ; if \; T = S \; (point \; doubling) \end{cases} \tag{5.6}$$

5.3 IMPLEMENTATION OF ELLIPTIC CURVE IN CRYPTOGRAPHY

For implementation of this curve in cryptography [1] the equation of elliptic curve is modified as:

$$(y^2) mod \, p \; = (x^3 + ax + b) \, mod \, p \tag{5.7}$$

With condition $4a^3 + 27b^2 \neq 0 \, mod \, p$, and $p > 3$, where p is a prime number.

This condition has geometrical significance that plot do not have self-intersections. The above equation is implemented by making calculation on both side of equation with modulo p and equating it for equal value..

Larger the value of p, more number of points will be available on elliptic curve to generate the key, hence more number of bits required to implement.

In cryptosystem we have a public key is represented as:

$$X = IT \tag{5.8}$$

Where I is the scalar value having value as integer, multiplied with the public key T which is also called generator which generates all the points on elliptic curve in cyclic order. The method of finding out this scalar value is known as Discrete Logarithm Problem [1], [2]. As subtraction is not possible on points on elliptic curve, once the point 3T is known then it is impossible to calculate 2T point or T point. Hence this scalar value is safe with single user only.

5.4 ANALOG IMPLEMENTATION OF THE ELLIPTIC CURVE

The expressed equation 5.1 can be implemented using the square root [3], cubic and linear blocks respectively. The circuit shown in Fig 5.3 provides us the analog implementation of elliptic curve which would be further used to calculate generator point and other points by applying several methods like Schoof's algorithm or Schoof-Elkies-Atkin algorithm, or Koblitz curves or complex multiplication techniques.

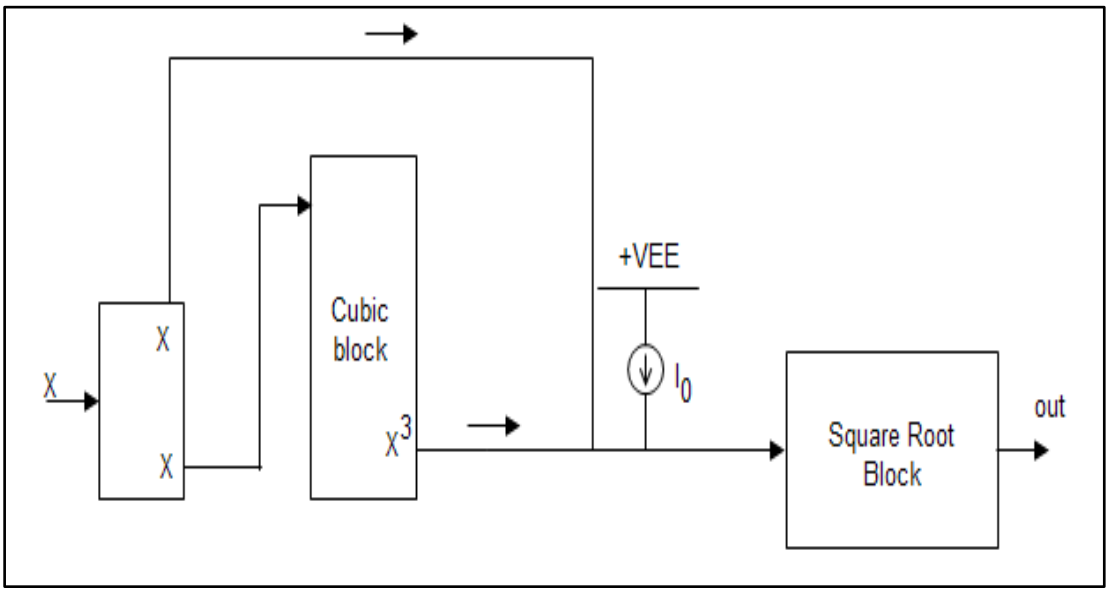

Fig 5.3 Elliptic Curve Generator Block

5.4.1 DC ANALYSIS OF ELLIPTIC CURVE

The DC analysis of this block for is done in PSPICE A/D for two different equations below:

i. For the value of a = -1 and b = 6 in equation 5.1 i.e. I_0 = 6uA and taking the negative coefficient linear term from linear block.

$$y^2 = x^3 - x + 6 \tag{5.9}$$

ii. For the value of a = 1 and b = 2 in equation 5.1, i.e. I_0 = 2uA and taking the positive coefficient linear term from linear block

$$y^2 = x^3 + x + 2 \tag{5.10}$$

The DC transfer characteristic for this block is shown in Fig 5.4 below with same biasing voltage of ±3.65V and input current ranging from -2uA to +4uA.

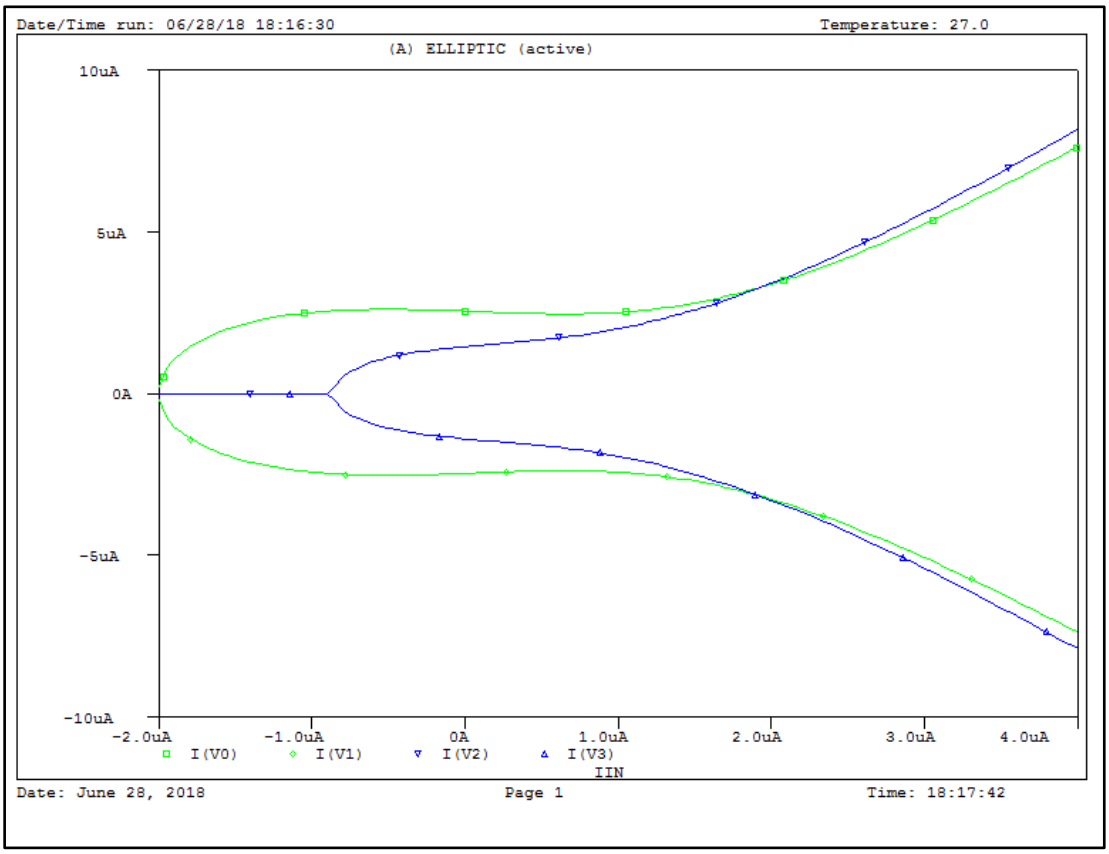

Fig 5.4 DC Transfer characteristic for Elliptic Curve

Here green color curve represents the first case whose equation is shown by equation number 5.9 and blue color curve represents the second case whose equation is shown by equation number 5.10.

5.4.2 COMPARISON WITH IDEAL ELLIPTIC CURVE

The comparison of elliptic curve is shown in Fig 5.5 below which is plotted in MATLAB where the blue color curve shows the simulated results and red

color the ideal results. The error graph is also shown in Fig 5.6 below where y-axis indicates the error and x-axis indicates the input current range.

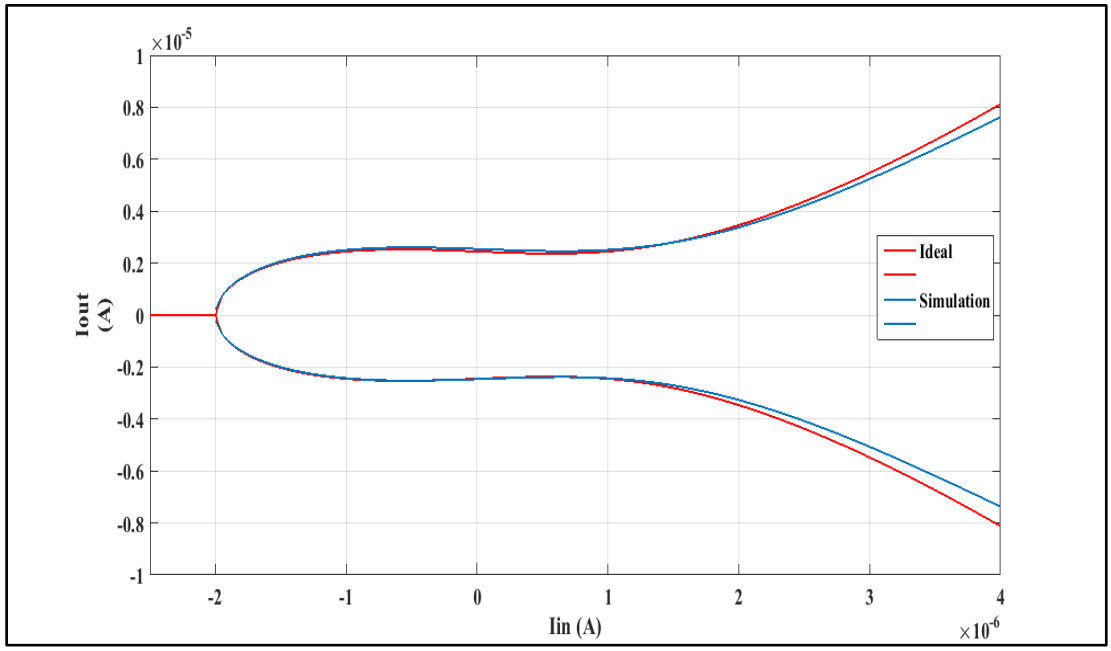

Fig 5.5 Comparison with Ideal elliptic curve

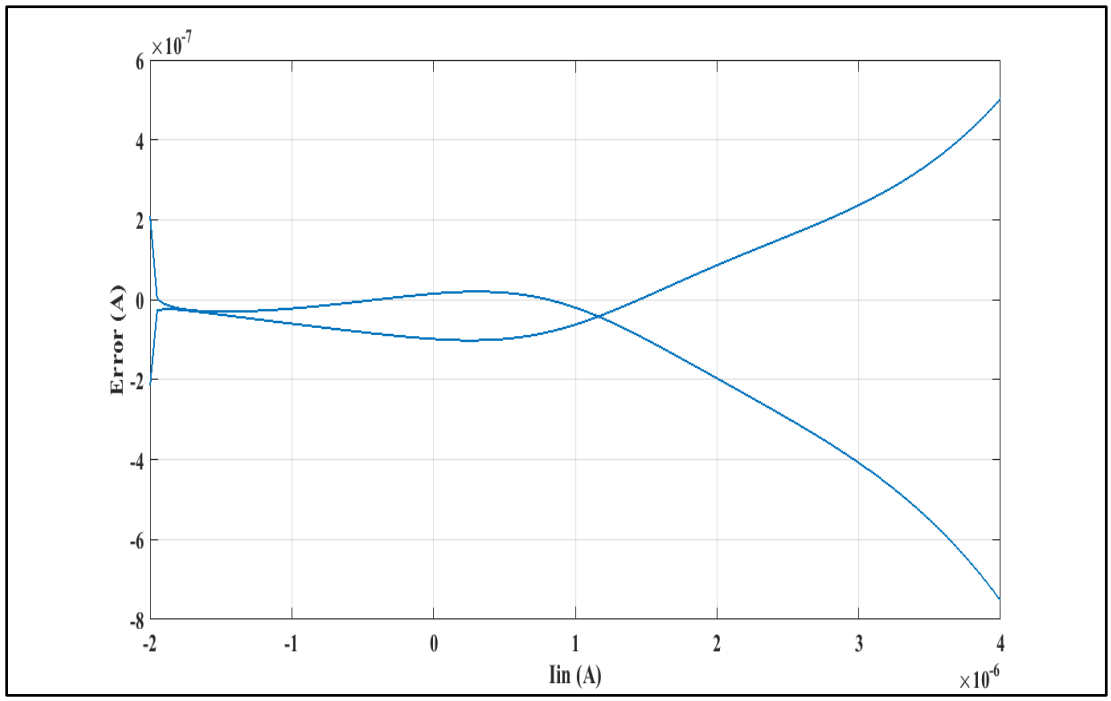

Fig 5.6 Error graph for Elliptic curve

The above Fig 5.6 shows that maximum deviation from the ideal value is 0.7uA at input value of 4uA i.e. 1.14% and minimum deviation is 0 % for input current value of -0.5uA and 0.9uA.

5.5 CONCLUSION

In this chapter we have presented an analog circuit implementation of the Elliptic Curve which may be used in Cryptography.

REFERENCES

[1] W. Stallings, Cryptography And Network Security Principles and Practices, *Prentice Hall*, 2012.

[2] S,.N. Kumar,"Review on Network Security and Cryptography," *International Transaction Of Electrical and Computer Engineers System*, 2015 3 (1), pp 1-11.

[3] M. Kumngern, K. Dejhan, "A New Translinear-Based Dual-Output Square-Rooting Circuit," *Active and Passive Electronic Components*, vol. 2008, Article ID 623970.

CHAPTER 6

SUMMARY AND FUTURE SCOPE

6.1 SUMMARY

In this dissertation, realization of non linear signal generating blocks is presented along with their implementation for attainment of non linear standard functions like Gaussian, sigmoid etc. as non linear signal generating blocks have become an important part in updated systems including biomedical, entertainment, defence, education and most important security.

In Chapter 1, the basics needed to understand that why analog signal processing is important, how analog signal processing is advantageous to digital implementation, how current mode is better than voltage mode, and lastly what is Cryptosystem and introduction to how elliptic curve can be used to enhance the security of information systems.

In Chapter 2, we have discussed about earlier research that has been done in this field of signal processing along with simulation in order to make more accurate blocks for further attainment of non linear functions.

In Chapter 3, realizations of non linear signal processing blocks that generates up to fifth order of terms with the help of bipolar transistor, their ideal and exact analysis done theoretically and along with comparison to their ideal behavior is shown, and the block's behavior to AC signal has been shown with their transient and AC analysis.

In Chapter 4, those blocks which were realized in the above chapter are used for attainment of some standard functions like Gaussian, sigmoid, trigonometric functions sine, cosine and tangent hyperbolic inverse, exponential and logarithmic.

The above functional circuits are realized in current mode and with the help of Taylor Series expansion.

In Chapter 5, we have implemented an analog signal processing circuit for the elliptic curve which may be used in Cryptography.

6.2 FUTURE SCOPE

In this dissertation, our major focus was on implementation of non linear functions and extends it to one of the application for security. As we have done bipolar implementation of those functional blocks, the non ideality was observed in results as we approximated our functions to the order of five. These block's result for higher order approximation can be made more close to ideal behavior with the implementation of more advanced bipolar transistors parameters.

APPENDICES

APPENDIX1

PSPICE model files used for 0.35 um technology of CMOS

*****Valid range for n channel and p channel models W ≥ 0.35um

*****Spice Level 7 Parameters

.MODEL NMOS1 NMOS LEVEL=7 MOBMOD=1 CAPMOD=2 NLEV=0 NOIMOD=1 K1=6.044E-1 K2=2.945E-3
+K3=1.72 K3B=6.325E-1 NCH=2.31E17 VTH0=4.655E-1 VOFF=5.72E-2 DVT0=2.227E+01 DVT1=1.051
+DVT2=3.93E-3 KETA=-6.21E-4 PSCBE1=2.756E8 PSCBE2=9.645E-6 DVT0W=0 DVT1W=0 DVT2W=0
+UA=1E-12 UB=1.723E-18 UC=5.756E-11 U0=4.035E2 DSUB=5E-1 ETA0=3.085E-2 ETAB=-3.95E-2
+NFACTOR=1.119E-1 EM=4.1E7 PCLM=6.831E-1 PDIBLC1=1.076E-1 PDIBLC2=1.453E-3 DROUT=5E-1
+A0=2.208 A1=0 A2=1 PVAG=0 VSAT=1.178E5 AGS=2.490E-1 B0=-1.76E-8 B1=0 DELTA=1E-2 PDIBLCB=2.583E-1
+W0=1.184E-7 DLC=4E-9 DWB=0 DWG=0 LL=0 LW=0 LWL=0 LLN=1 LWN=1 WL=0 WW=0 WWL=0 WLN=1 WWN=1 AT=3.3E4
+UTE=-1.8 KT1=-3.3E-1 KT2=2.2E-2 KT1L=0 UA1=0 UB1=0 UC1=0 PRT=0 CGDO=1.12E-10 CGSO=1.12E-10
+CGBO=1.1E-10 CGDL=1.35E-10 CGSL=1.35E-10 KAPPA=6E-1 CF=0 ELM=5 XPART=1 CLC=1E-15
+CLE=6E-1 RDSW=6.043E2 CDSC=0 CDSCB=0 CDSCD=8.448E-5
+PRWB=0 PRWG=0 CIT=1E-3 TOX=7.7E-9 NGATE=0 NLX=1.918E-7 ALPHA0=0 BETA0=3E1 AF=1.4 KF=2.810E-27
+EF=1 NOIA=1E20 NOIB=5E4 NOIC=-1.4E-12 LINT=-1.67E-8 WINT=2.676E-8 XJ=3E-7 RSH=8.2E1 JS=2E-5
+CJ=9.3E-4 CJSW=2.8E-10 CBD=0 CBS=0 IS=0 MJ=3.1E-1 N=1 MJSW=1.9E-1 PB=6.9E-1 TT=0 PBSW=6.9E-1.

.MODEL PMOS1 PMOS LEVEL=7 MOBMOD=1 CAPMOD=2 NLEV=0 NOIMOD=1 K1=5.675E-1 K2=-4.39E-2
+K3=4.54 K3B=-8.52E-1 NCH=1.032E17 VTH0=-6.17E-1 VOFF=-1.13E-1 DVT0=1.482 DVT1=3.884E-1
+DVT2=-1.15E-2 KETA=-2.56E-2 PSCBE1=1E9 PSCBE2=1E-8 DVT0W=0 DVT1W=0 DVT2W=0

+UA=2.12E-10 UB=8.29E-19 UC=-5.28E-11 U0=1.296E2 DSUB=5E-1 ETA0=2.293E-1 ETAB=-3.92E-3
+NFACTOR=8.237E-1 EM=4.1E7 PCLM=2.979 PDIBLC1=3.310E-2 PDIBLC2=1E-9 DROUT=5E-1
+A0=1.423 A1=0 A2=1 PVAG=0 VSAT=2E5 AGS=3.482E-1 B0=2.719E-7 B1=0 DELTA=1E-2 PDIBLCB=-1.78E-2
+W0=4.894E-8 DLC=4E-9 DWB=0 DWG=0 LL=0 LW=0 LWL=0 LLN=1 LWN=1 WL=0 WW=0 WWL=0 WLN=1 WWN=1 AT=3.3E4
+UTE=-1.35 KT1=-5.7E-1 KT2=2.2E-2 KT1L=0 UA1=0 UB1=0 UC1=0 PRT=0 CGDO=7.42E-11 CGSO=7.42E-11
+CGBO=1.1E-10 CGDL=1.29E-10 CGSL=1.29E-10 KAPPA=6E-1 CF=0 ELM=5 XPART=1 CLC=1E-15
+CLE=6E-1 RDSW=1.853E3 CDSC=6.994E-4 CDSCB=2.943E-4 CDSCD=1.97E-4
+PRWB=0 PRWG=0 CIT=1.173E-3 TOX=7.7E-9 NGATE=0 NLX=1.77E-7 ALPHA0=0 BETA0=3E1 AF=1.29 KF=1.090E-27
+EF=1 NOIA=1E20 NOIB=5E4 NOIC=-1.4E-12 LINT=-8.14E-8 WINT=3.845E-8 XJ=3E-7 RSH=1.56E2 JS=2E-5
+CJ=1.420E-3 CJSW=3.8E-10 CBD=0 CBS=0 IS=0 MJ=5.5E-1 N=1 MJSW=3.9E-1 PB=1.02E0 TT=0 PBSW=1.02E0.

.....

PSPICE Model file for Bipolar Transistors NR200N and PR200N.

*****Transistor array: ALA400
*Company: AT&T

.....

.MODEL NR200N NPN RB=262.5 IRB=0 RBM=12.5 RC=25 RE=0.5
+IS=242E-18 EG=1.206 XTI=2 XTB=1.538 BF=137.5
+IKF=13.94E-3 NF=1 VAF=159.4 ISE=72E-16 NE=1.713
+BR=0.7258 IKR=4.396E-3 NR=1 VAR=10.73 ISC=0 NC=2
+TF=0.425E-9 TR=0.425E-8 CJE=0.428E-12 VJE=0.5
+MJE=0.28 CJC=1.97E-13 VJC=0.5 MJC=0.3 XCJC=0.065
+CJS=1.17E-12 VJS=0.64 MJS=0.4 FC=0.5.

.MODEL PR200N PNP RB=163.5 IRB=0 RBM=12.27 RC=25 RE=1.5
+IS=147E-18 EG=1.206 XTI=1.7 XTB=1.866 BF=110
+IKF=4.718E-3 NF=1 VAF=51.8 ISE=50.2E-16 NE=1.650
+BR=0.4745 IKR=12.96E-3 NR=1 VAR=9.96 ISC=0 NC=2
+TF=0.610E-9 TR=0.610E-8 CJE=0.36E-12 VJE=0.5
+MJE=0.28 CJC=0.328E-12 VJC=0.8 MJC=0.4 XCJC=0.074
+CJS=1.39E-12 VJS=0.55 MJS=0.35 FC=0.5.

.....

APPENDIX2

Dimensions of CMOS Transistors used in Fig 2.2:

Table 2: W/L Ratio for CMOS Linear and Squarer Circuit for long channel length

Transistors	W/L (µm/µm)
M1-M2	10/2
M3-M4	10/1
M5	10/1
M6-M7	10/2
M8	10/1
M9	20/1
M10	10/1

Table 3: W/L ratio for CMOS Linear and Squarer circuit for Short Channel Length

Transistors	W/L (µm/µm)
M1-M2	1/1
M3-M4	1/0.5
M5	1/0.5
M6-M7	1/1
M8	1/0.5
M9	0.5/0.5
M10	1/1

Dimensions for CMOS transistors used in Fig 2.15

Table 4: W/L Ratio for CMOS Square Rooting Block

Transistors	W/L (μm/μm)
M1-M4	100/10
M5	25/10
M6-M7	100/10

Dimensions for CMOS transistors used in Fig. 2.17

Table 5: W/L Ratio for CMOS Sigmoid Function Generator

Transistors	W/L (μm/μm)
M1	2.12/0.4
M2	1.08/0.4
M3	1.6/0.4
M4	0.52/0.4
M5	1.6/0.4
M6	0.52/0.4