İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

CHAOTIC OSCILLATOR BASED RANDOM BIT GENERATOR

M.Sc. Thesis by

Erdoğan Özgür ATEŞ, B.Sc.

Department: **Electronics and Communication Engineering**

Programme: **Electronics Engineering**

MAY 2005

İSTANBUL TECHNICAL UNIVERSITY ★ INSTITUTE OF SCIENCE AND TECHNOLOGY

CHAOTIC OSCILLATOR BASED RANDOM BIT GENERATOR

M.Sc. Thesis by

Erdoğan Özgür ATEŞ, M.Sc.

(504021206)

Date of submission : 9 May 2005

Date of defence examination: 30 May 2005

Supervisor (Chairman): Assoc. Prof. Dr. Ali ZEKİ

Members of the Examining Committee Assoc. Prof. Dr. Serdar ÖZOĞUZ

Assist. Prof. Dr. A. Şima ETANER-UYAR

MAY 2005

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KAOTİK OSİLATÖR TABANLI RASGELE SAYI ÜRETECİ

YÜKSEK LİSANS TEZİ

Müh. Erdoğan Özgür ATEŞ

Tezin Enstitüye Verildiği Tarih : 9 Mayıs 2005

Tez Danışmanı : **Doç.Dr. Ali ZEKİ**

Diğer Jüri Üyeleri **Doç. Dr. Serdar ÖZOĞUZ**

Yrd. Doç. Dr. A. Şima ETANER-UYAR

MAYIS 2005

ACKNOWLEDGEMENT

I would like to thank my supervisor Assoc. Prof. Dr. Ali Zeki who has supported me during B.Sc. and M.Sc. education and M.Sc. thesis.

I would like to thank Assoc. Prof. Dr. Serdar Özoğuz for his assistance and support efforts.

In this work, test chip is submitted with research budget of Assoc. Prof. Dr. Serdar Ozoguz who is awarded by TÜBA's (Türkiye Bilimler Akademisi) Young Scientists Award Programme (TÜBA-GEBİP). I would like to thank again Assoc. Prof. Dr. Serdar Ozoguz and Türkiye Bilimler Akademisi for their support.

I am very grateful to ETA ASIC Design Center for hardware and software support throughout designing processes.

I am very grateful to my colleagues in ETA ASIC Design Center who have supported me during my thesis, and helped me with their valuable advises.

I feel obliged to dedicate my thesis to my family, who encouraged and supported me while I was taking my steps at each stage of my life upon.

Finally, I would like to thank Tülay Yaşar for her endless support and love.

Last, but not the least, I would like to thank to all my professors at ITU, I could not have become an engineer without their education.

May 2005 Erdoğan Özgür Ateş

CONTENTS

TABLE LIST

FIGURE LIST

Page No

KAOTİK OSİLATÖR TABANLI RASGELE SAYI ÜRETECİ

ÖZET

Bu çalışmada, yüksek hızlı, sürekli zaman kaotik osilatörü tasarlanmış ve rasgele bit üretiminde kullanılmıştır. Yüksek hızlı sürekli zaman kaotik osilatörü literatürde çokça kullanılmakta olan negatif iletkenlikli LC sinüs osilatör devresinden türetilmiştir. Spectre spice simülatörü kullanılarak elde edilen bilgiler ışığında, tasarlanan sürekli zaman kaotik osilatörünün GHz frekanslarında çalışabildiği tespit edilmiştir. Rasgele bit üreteci blokları Emetör Bağlamalı Lojik ve Akım Modlu Lojik aileleri kullanılarak tasarlanmıştır. Bu lojik ailelerle yüksek frekanslarda çalışan sayısal devrelerin gerçeklenmesi mümkündür ve güç hattı gürültülerinden daha az etkilenmektedirler. Spectre simülatöründe gerçekleştirilen simülasyonlar, tasarlanan rasgele bit üretecinin 300Mbit/s hızında çıkış oluşturabildiğini göstermiştir. Rasgele sayı üretiminde ihtiyaç duyulan fark alma işlemi için, açık çevrimde çalışan emetör dejenerasyonlu fark alıcı devre kullanılmıştır. Bipolar emetör dejenerasyonlu farksal kuvvetlendirici kullanılarak, GHz frekanslarında çalışan fark alıcı devreler gerçeklenebildiği Spectre simülasyonlarıyla gösterilmiştir. PMOS transistorlar ve polisilikon dirençler kullanılarak GHz frekanslarında çalışabilen tümleştirilmiş ayarlanabilir direnç yapısı gerçeklenmiş, proseste meydana gelebilecek değişimlerle direnç değerlerinin sapmasını engellemek amacıyla bu yapının kullanılabileceği gösterilmiştir. Yapıdaki PMOS transistorların geçit kontrol gerilimini otomatik olarak üreten devre gerçeklenmiştir. Akım Modlu Lojik Giriş Çıkış Pad Sürücü devreleri, kırmıktaki çıkış bloklarını sürmek amacıyla tek uçlu 400mV_{pp} salınım sağlayacak şekilde tasarlanmıştır. Kaotik osilatör ve rasgele bit üreteci sistemi, IHP SGB25VD 0.25µm SiGeC BiCMOS prosesi ile gerçeklenmiştir. Kaotik osilatör ve rasgele bit üreteci blokları 48mW güç harcamaktadırlar. Toplam kırmık alanı 1 mm x 0.5 mm'dir.

CHAOTIC OSCILLATOR BASED RANDOM BIT GENERATOR

SUMMARY

In this study, a high speed continuous time chaotic oscillator is designed and utilized as a random bit generator. High speed continuous time chaotic oscillator is derived from well known negative-gm LC sinus oscillator. From Spectre simulations, it is verified that used chaotic oscillator can operate at several GHz frequencies. Random bit generation blocks are implemented with bipolar Emitter Coupled Logic and Current Mode Logic circuits which are superior for high frequency operation and better supply noise rejection. Spectre simulations show that designed random bit generator's average throughput is 300Mbit/s. An open-loop emitter degenerated difference amplifier is used for difference operation. Spectre simulations verify that it is possible to realize difference amplifier operating at GHz frequency range by using bipolar emitter degenerated differential pair amplifier. An integrated tunable resistor that can operate at GHz frequencies is implemented with PMOS transistors and polysilicon resistors to overcome resistance value deviations due to process variations. Automatic tuning circuit is also realized for generating correct source-gate voltage for PMOS transistor in the structure. Current Mode Logic Input Output Pad drivers with single ended $400mV_{pp}$ swing are designed to drive output pads of the circuit. Chaotic oscillator and random bit generator system is implemented with IHP's SGB25VD 0.25µm SiGeC BiCMOS process. Chaotic oscillator and random bit generator block consumes 48mW power under typical conditions. Total area of the chip is 1 mm x 0.5 mm.

1. INTRODUCTION

1.1 Random Numbers

Random number generators are used in many areas including computer simulations, Monte Carlo techniques, statistical analysis and cryptography. A good random number generation helps to improve the results in these applications and is vital for cryptographic security. The security of cryptographic algorithms depends on generating secret keys which are generated by random number generators. Random number generator is a device or algorithm whose output is a sequence of statistically independent and unbiased binary digits. To make sure that a random number generator (RNG) is secure, its output must be indistinguishable from a true random sequence and unpredictable.

RNGs can be classified into two classes which are true random number generators (TRNG) and pseudo random number generators (PRNG). A TRNG operates by measuring unpredictable natural processes such as thermal noise from a semiconductor, frequency instability of an oscillator, elapsed time between emission of particles during radioactive decay and variations in disk drive response times. The processes produce continuous time analog signals which are often called noise. PRNGs use deterministic processes to generate a series of outputs from an initial seed state [1].

1.2 Chaos

Chaos is whether or not to make accurate long term predictions about the future of the system. The output of the chaotic systems can be predicted from the exact initial conditions depending on the first Lyapunov exponent. However, sensitivity with respect to the initial conditions causes unpredictability on the long term.

Chaos theory was formulated during the 1960s. The name chaos was coined by Jim Yorke, an applied mathematician at the University of Maryland. In 1961, Edward Lorentz discovered the butterfly effect while trying to forecast the weather. He was

running a long series of computations on a computer when he decided he needed another run. Rather than do the entire run again, he decided to save some time by typing in some numbers from a previous run. Later, when he looked over the printout, he found an entirely new set of results. The results should have been the same as before. After thinking about this unexpected result, he discovered that the numbers he typed in had been slightly rounded off. In principle, this tiny difference in initial conditions should not have made any difference in the result, but it did. From this, Lorentz determined that long-distant weather forecasts are impossible to predict. Tiny differences in weather conditions, on any one day, will show dramatic differences, after a few weeks, and these differences are entirely unpredictable. Although Lorentz's discovery was an accident, it planted the seed for the new theory of chaos science.

Chaos was first observed electronically in Chua's circuit. Chaotic nature of Chua's circuit was first observed by Matsumoto in 1983 using computer simulations, following the instructions of Chua, who had invented this circuit and had explained its operating principles to Matsumoto moments before he was rushed to a hospital for a major surgery, and who did not participate in the early phases of this research. In acknowledging his subsidiary role as a computer programmer, Matsumoto had named this circuit Chua's circuit. The first experimental Chua's circuit which confirms the presence of chaos was due to Zhong and Ayrom in 1984 [2].

The divergence of trajectories associated with chaos, along with the inclusion of noise, renders sequences unpredictable to an extent, qualifying the system to be used as a truly random bit source.

1.3 Organization of Thesis

The goal of this thesis is designing a high speed continuous time chaotic oscillator and utilizing it to implement a high speed random bit generator.

Chapter 2 is a review of randomness. Random number generators, randomness tests are explained in detail. Integrated circuit implemented random number generators are given.

Chapter 3 is a review of chaos theory. Chua's circuit is explained as an example of chaos in electronic systems.

Chapter 4 is the major subject of the thesis. Designed high speed chaotic oscillator is explained in detail. Random bit generator system is presented and discussed in detail.

Chapter 5 is about circuit level design of chaotic oscillator and random bit generator system. Designed circuits are explained in detail. Simulation results of each component and entire design are presented.

Chapter 6 is a review of the thesis and conclusion is given.

2. RANDOM NUMBER GENERATORS

2.1 Introduction

Random numbers are statistically independent and unbiased sequence of digits that have high rate entropy. They are used in computer simulations, Monte-Carlo techniques in numerical analysis, test pattern generation for performance analysis of systems and cryptography. Security systems that are built on cryptographic algorithms need real random numbers to prevent attacks. Security processes that lack adequate sources of randomness will have poor security [1].

A random bit generator is a device or algorithm which outputs a sequence of statistically independent and unbiased binary digits. The quality of a random number generator is often measured by the degree to which it produces unpredictable and unbiased output. A random integer can be obtained by generating a random number bit sequence and converting it to an integer. There are two kinds of random number generators: [3]

1. Pseudorandom Number Generators
2. Real Random Number Generators

2.2 Pseudo Random Number Generators:

A pseudorandom bit generator (PRBG) is a deterministic algorithm which outputs a binary sequence that appears to be random. Input to the PRBG is called the seed, while the output of the PRBG is called a pseudorandom bit sequence.

The output of a PRBG is not random. Their outputs are predictable and hence entirely insecure for cryptographic applications. They can be used to further improve a real random number generator output or convert the real number generators output to a specific length of binary digits. Such generators are also commonly used for simulation purposes. They can pass randomness tests. ANSI X9.17 and FIPS 186 generator are examples of pseudorandom number generators [3].

2.3 Real Random Number Generators

A true random number generator requires a naturally source of randomness. Designing a hardware device or software program to exploit this randomness and produce a bit sequence is a difficult task. Random number generators based on natural sources of randomness are subject to influence by external factors. Therefore it is important to test such devices periodically. True random numbers can be obtained by using hardware-based or software-based techniques.

2.3.1 Hardware-based Generators

Hardware-based random bit generators make use of the randomness of some physical occurrence. Such physical processes may produce bits that are biased and correlated, in which case they should be processed with de-skewing techniques. Examples of natural randomness sources are:

- Elapsed time between emission of particles during radioactive decay,
- Thermal noise from a semiconductor diode or resistor,
- The frequency instability of a free running oscillator,
- The amount a metal-insulator-semiconductor capacitor is charged during a fixed period of time,
- Air turbulence within a sealed disk drive which causes random fluctuations in disk drive sector read latency times, and
- Sound from a microphone, or video output from a camera.

2.3.2 Software-based Generators

Designing a random bit generator in software is even more difficult than doing so in hardware. Processes which software random bit generators are based upon include:

- The system clock,
- Elapsed time between keystrokes or mouse movement,
- Content of input/output buffers,
- User input, and

- Operating system values such as system load or network statistics.

2.3.3 De-skewing

A natural source of random bits output maybe biased (the probability of the producing a 1 is not equal to $\frac{1}{2}$) or correlated (the probability of the generated output bit depends on previous bits). Techniques for generating true random numbers from such a natural source's output are called de-skewing.

Suppose that a generator produces biased but uncorrelated bits. If the output sequence of such a generator is grouped into pairs of bits, with a 10 pair transformed to a 1, a 01 pair transformed to a 0, and 00 and 11 pairs are discarded, then the resulting sequence is both unbiased and uncorrelated. This technique is invented by Hungarian mathematician Jon Von Neumann [3].

2.4 Statistical Tests

Statistical tests are designed to measure the quality of a number generator claimed to be random. It is impossible to give a mathematical proof that a generator is a random number generator and statistical tests only help to detect generator's weaknesses. This is accomplished by taking a sample output sequence of the generator and applying statistical tests to this sequence. Each statistical test determines whether the sequence has certain attributes like a truly random sequence would likely to exhibit. If the sequence fails any one of the tests, the generator may be rejected as being non-random. On the other hand, if the sequence passes all of the tests, the generator is accepted as being random.

2.4.1 Monobit test

The purpose of this test is to determine whether the number of 0's and 1's are approximately same as would be expected from a random sequence. Let n_0, n_1 indicate the number of 0's and 1's in sequence s, respectively. Monobit test outcome X_1 is defined by equation (2.1b).

$$n_0 + n_1 = n \tag{2.1a}$$

$$X_1 = \frac{(n_0 - n_1)^2}{n} \tag{2.1b}$$

2.4.2 Serial Test

The purpose of this test is to determine whether the number of occurrences of 00, 01, 10 and 11 as subsequences of s are same, as would be expected for a random sequence. Let n_0, n_1 denotes number 0's and 1's in s, respectively, and let $n_{00}, n_{01}, n_{10}, n_{11}$ denote the number of occurrences of 00, 01, 10 and 11 in s, respectively. Serial test outcome X_2 is defined by equation (2.2).

$$X_2 = \frac{4}{n-1}(n_{00}{}^2 + n_{01}{}^2 + n_{10}{}^2 + n_{11}{}^2) - \frac{2}{n}(n_0{}^2 + n_1{}^2) + 1 \tag{2.2}$$

2.4.3 Poker Test

Let m be a positive integer such that $\left\lfloor \frac{n}{m} \right\rfloor \geq 5 \cdot (2^m)$, and let $k = \left\lfloor \frac{n}{m} \right\rfloor$. Divide the sequence s into k non-overlapping parts each of length m, and let n_i be number of occurrences of the i^{th} type of sequence of length m, $1 \leq i \leq 2^m$. The poker test determines whether the sequences of length m each appear approximately the same number of times in s, as would be expected for a random sequence. Poker test outcome X_3 is defined by equation (2.3).

$$X_3 = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^2\right) - k \tag{2.3}$$

2.4.4 Runs Test

The purpose of the runs test is to determine whether the number of runs of either zeros or ones of various lengths in the sequence s is as expected for a random sequence.

2.4.5 FIPS 140-1 Statistical Test for Randomness

Federal Information Processing Standards (FIPS 140-1) specifies four statistical tests for randomness. FIPS-140-1 is issued by the National Institute of Standards and Technology (NIST). A single bit string s of length 20000 bits, output from a generator, is subjected to each of the following tests. If any of the tests fail, then the generator fails the test.

2.4.5.1 Monobit Test

The number of 1's in sequence s should satisfy $9654 < n_1 < 10346$.

2.4.5.2 Poker Test

The statistic X_3 defined in equation 3 is computed for $m = 4$. The poker test is passed if $1.03 < X_3 < 57.4$.

2.4.5.3 Runs Test

The number of blocks and gaps, respectively, of length i in s are counted for each i, $1 < i < 6$. The runs test is passed if runs are each within the corresponding interval specified by the following table.

2.4.5.4 Long Run Test

The long run test is passed if there are no runs of length 34 or more [3].

Tablo 2.1: Long runs

Length of run	Required Interval
1	2267 - 2733
2	1079 - 1421
3	502 – 748
4	223 – 402
5	90 – 223
6	90 - 223

2.5 IC Implemented Random Number Generators

The expanding use of digital communications by way of computer networks, the Internet, and wireless devices has resulted in a greater need for the protection of transmitted information using cryptography. Cryptography allows for the private exchange of authentic messages between a sender and a receiver using carefully generated and distributed cryptographic keys for encryption and decryption. The security of most cryptographic systems relies on the generation of unpredictable and irreproducible digital keystreams using a nondeterministic random number generator (RNG). As system-on-a-chip solutions become more widespread, robust integrated-circuit (IC) RNG designs will be needed for secure communication applications.

2.5.1 Noise-Based IC Random Number Generators

Random noise sources, such as thermal and shot noise, exist at the IC level but are often masked by deterministic disturbances. Consequently, commercial RNG designs that amplify electronic noise require external components and special hardware for electromagnetic shielding from nonrandom interferences. Substrate noise and power supply noise levels are often much higher than random noise levels in typical integrated systems. Consequently, methods capable of producing random sequences using corrupted noise sources must be employed in noise-based IC random number generators. Different noise-based IC random number generators can be classified as: direct amplification, oscillator sampling and chaos based [4].

2.5.1.1 Direct Amplification

The direct amplification technique shown in Figure 2.1 uses a high-gain high-bandwidth amplifier to process the small ac voltage produced by a noise source such as thermal or shot noise. The noise must be amplified to a level where it can be accurately processed with no bias by a clocked comparator. This is the most popular RNG technique for single-chip solutions where shielding of the noise source is possible. The lack of adequate shielding from power supply and substrate signals in an IC environment prohibits the exclusive use of this method for IC-based cryptographic systems [5].

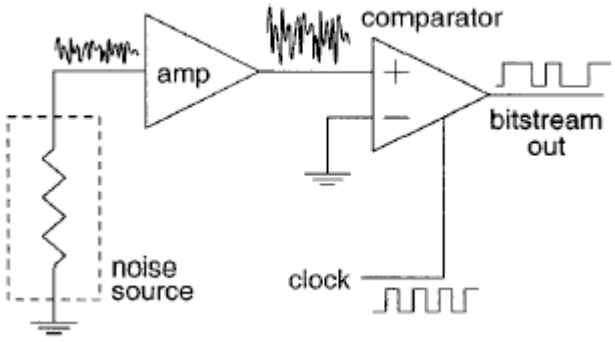

Figure 2.1: Direct noise amplification technique

2.5.1.2 Oscillator Sampling

The oscillator sampling method produces randomness from phase noise in free-running oscillators. An example of this technique is shown in Figure 2.2, where the output of a fast oscillator is sampled on the rising edge of a slower clock using a D flip-flop. Oscillator jitter (i.e., cycle-by-cycle variations in the oscillator's period) is

causes uncertainty in the exact sample values, ideally producing a random bit for each sample. Additionally, randomness is artificially enhanced by carefully selecting the ratio of the fast and slow oscillator frequencies. Pseudorandom techniques are added to further randomize the output in case of oscillator jitter levels are not enough to produce randomness, potentially compromising the unpredictability of the system.

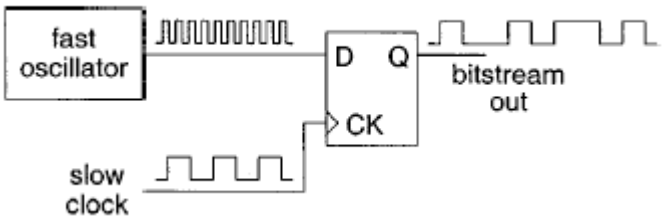

Figure 2.2: Oscillator Sampling

2.5.1.3 Chaos Based Integrated Random Generators

Chaotic systems can be implemented electronically using analog or digital circuit techniques. The divergence of trajectories associated with chaos, along with the inclusion of noise, renders sequences unpredictable to an extent, qualifying the system to be used as a truly random bit source [4].

A deterministic system is called chaotic if an infinitesimally small perturbation to its initial conditions produces a change in its behavior that grows exponentially with time. This phenomenon is numerically simulated from a chaos generation system and shown in Figure 2.3. While chaos is a concept completely different from randomness, it is important in random-number generation. If an RNG is chaotic, and if there is some inescapable uncertainty in any contribution to its state (e.g., due to thermal noise), then simply by waiting for a certain length of time, namely the time required for the exponential growth of that uncertainty to reach the magnitude of the system's gross state, one can assume that the state of the system is unknowable. By waiting a sufficient length of time between samplings, it may be possible to sample high-quality random bits from a chaotic system that is otherwise deterministic [6].

2.5.2 Integrated Random Number Generators Based on MOS (Metal Oxide Semiconductor) Structure

High quality random number generators can be generated by large fluctuating current of MOS capacitors after soft breakdown. It is known that when soft breakdown occurs in silicon dioxide thin film, a large fluctuation signal is observed for the

leakage current through the film. Larger variation of signals has advantages for converting them into random numbers. Once soft breakdown occurs in MOS structure, the currents change abruptly and vary randomly. It is thought that the current fluctuation is a consequence of the interaction between defects formed by high energy electrons in the insulating film and electrons conducting through the film.

A random number generator that uses MOS soft breakdown as randomness source shown in Figure 2.4 is implemented in [7] and achieves 50 kbits/s bit rate. An astable multivibrator output period is determined by resistances and capacitances in the circuit. One of the resistances is replaced by MOS structure that is operating in soft breakdown and as a result output period of astable multivibrator is fluctuating. To further improve statistical characteristics of random number generator, additional circuits might be used after this structure.

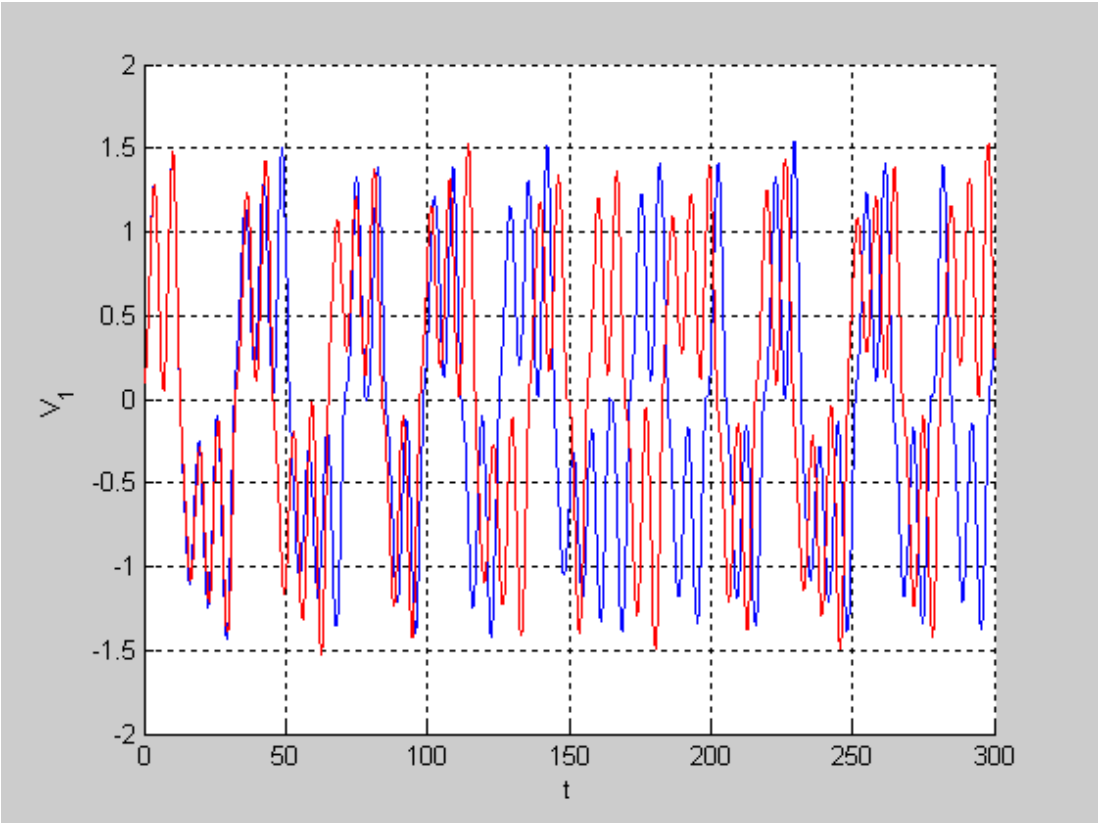

Figure 2.3: A small perturbation on initial conditions change behavior of the same chaotic system that grows exponentially

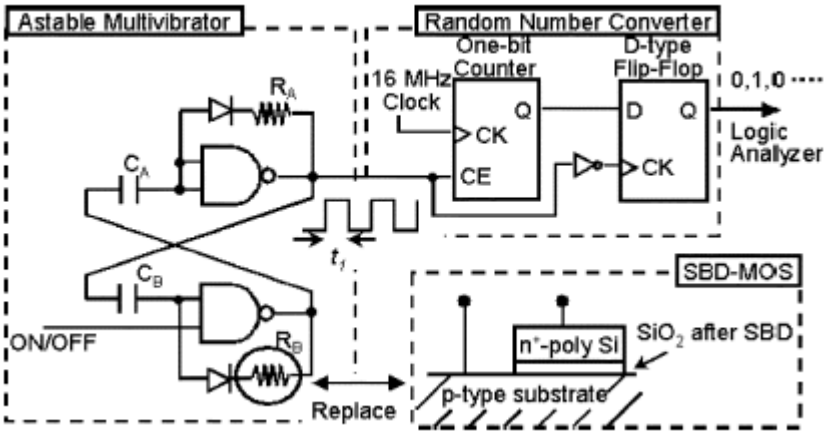

Figure 2.4: Schematic diagram of the random number generator based on MOS soft breakdown

3. CHAOTIC OSCILLATORS

Chaos refers to whether or not it is possible to make accurate long-term predictions about the behavior of the system. Chaotic nature is very sensitive to initial conditions of the system's state. No measurement can be made with infinite accuracy, therefore chaotic systems' output can not be determined previously. By definition, the vector field of an autonomous system is a unique function and is therefore unique at every point X in the state space. An important consequence of this is that a trajectory of the system cannot go through the same point twice, and therefore system's output is nonperiodic [8].

Design of electronic circuits with chaotic behavior has potential interest in many applications such as instrumentation, analog signal processing, communication and ranging systems. Regarding instrumentation, chaotic circuits represent an efficient alternative for nonrepeatable pseudorandom signal generation. Such generators are useful for the implementation of noise sources which are frequently employed at speech processing and for testing the dynamic behavior of electronic systems. On the other hand, chaos generators can be used in analog signal processing applications as a dither source to improve the performance of other blocks. For instance, dithering can be used to whiten the noise floor of $\sum\Delta$ modulators, as well as to reduce the idle channel spurious tones, which are introduced during quantization of direct current (DC) inputs. Also, dithering can be used to improve the integral nonlinearity of high performance Nyquist-rate analog to digital converters. In ranging systems, the nonperiodicity of chaotic signals makes chaos an interesting coding system for high resolution radar systems. Finally, chaotic circuits play a leading role in chaos-based digital communication systems.

Chaotic circuits can be realized by interconnecting discrete integrated circuit component parts on a printed circuit board. In order to decrease dimensions of circuits, power consumption and increase operating speed, chaotic circuits must be realized as monolithic ICs where they can be embedded with other analog and digital circuits.

Every mathematical model able to produce chaotic behavior has two features: dynamics and nonlinearity. Regarding dynamics, models for chaos generation can be

classified into discrete-time and continuous-time, depending on whether the system is described by nonlinear difference or differential equations, respectively. Another possible classification is autonomous or nonautonomous systems, which depends on whether the generator is able or not to self-sustain chaotic oscillations without any external excitation. Autonomous discrete-time systems can be generally described by the following qth (delay) order n-dimensional finite-difference equation,

$$x(k+q) = F[x(k+q-1),...,x(k)] \tag{3.1}$$

where $k = 0,1,2,...$ symbolizes the discrete time variable, x(k) represents the state vector of the system at the k th discrete time instant and F is a n-dimensional time-invariant vector field. Autonomous continuous-time ODE (Ordinary Differential Equations) based chaos generators are defined by the state equations,

$$\frac{dx(t)}{dt} = F(x(t)) \tag{3.2}$$

where $x(t)$ is the state vector of the system (also trajectory) and F is the nonlinear vector field that defines the direction and speed of a trajectory at every point in the state space and at every instant of time [9].

In order to exhibit chaos electronically, an autonomous circuit consisting of resistors, capacitors, and inductors must contain

1. at least one nonlinear element
2. at least one locally negative resistor
3. at least three energy-storage elements.

Chua's circuit is the simplest electronic circuit that satisfies these criteria. It is mathematically and experimentally proven that this circuit exhibit chaos.

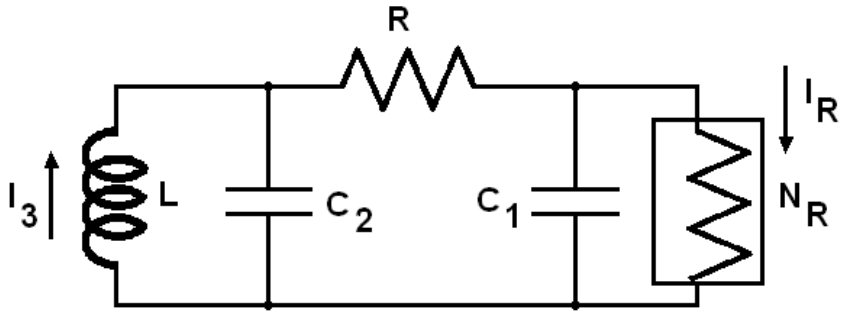

Figure 3.1: Chua's circuit

Chua's circuit shown in Figure 3.1 consist of a linear inductor L, a linear resistor R, two linear capacitors C1 and C2 and a single voltage controlled nonlinear resistor called Chua's diode [8].

The state equations of Chua's circuit are:

$$\frac{dv_1}{dt} = \frac{1}{C_1}\left[G(v_2 - v_1) - f(v_1)\right] \tag{3.3}$$

$$\frac{dv_2}{dt} = \frac{1}{C_2}\left[G(v_1 - v_2) + i_3\right] \tag{3.4}$$

$$\frac{di_3}{dt} = -\frac{1}{L}v_2 \tag{3.5}$$

where

$$G = \frac{1}{R} \tag{3.6}$$

and

$$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)\left\{|v_1 + E| - |v_1 - E|\right\} \tag{3.7}$$

is the $v - i$ characteristic of Chua's diode shown in Figure 3.2. [2].

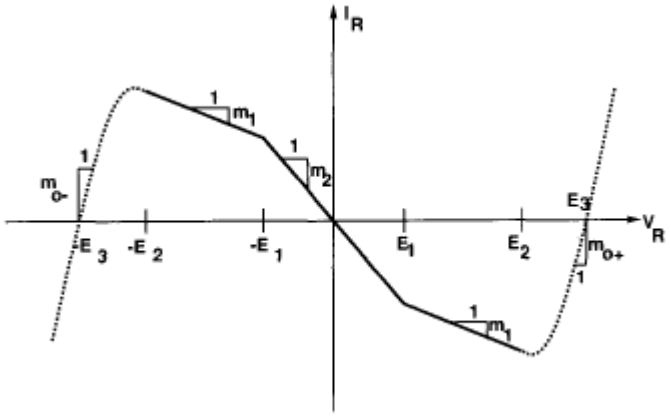

Figure 3.2: Driving point characteristic of Chua's diode

For a fixed set of parameters, the Chua's oscillator equations described above define a dynamical system which acts in a certain manner. For example, trajectories could converge to an equilibrium point, a limit cycle or an attractor. An equilibrium point could be stable or unstable. Chaotic attractor obtained from numerical simulation of Chua's circuit with proper parameters is shown in Figure 3.3.

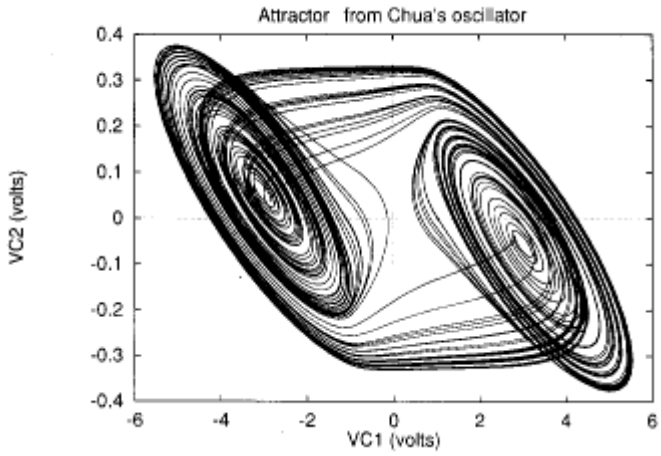

Figure 3.3: Chaotic attractor obtained from numerical simulation of Chua's circuit

In any analog continuous-time chaotic oscillator, there exists a core oscillator providing an unstable pair of complex conjugate eigenvalues and a control parameter which can move this pair. In the case of Chua's circuit, core oscillator is LC resonant oscillator [10].

4. HIGH SPEED INTEGRATED LC CHAOTIC OSCILLATOR AND ITS APPLICATION TO RANDOM NUMBER GENERATOR

In this work, a high speed chaotic oscillator and its random number generator block are studied. For random number generation, method in [1] is used. System used for random number generation from double scroll chaotic oscillator in [1] is shown in Figure 4.1.

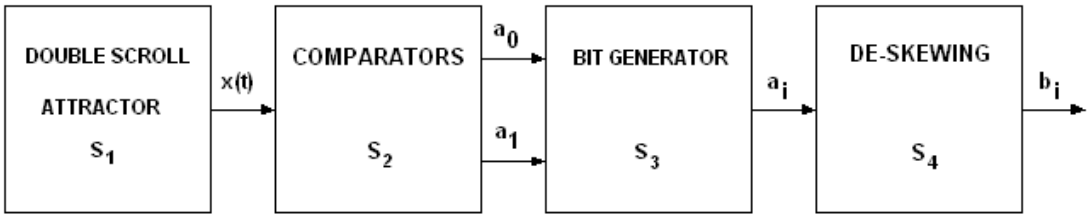

Figure 4.1: System of random number generation from double scroll chaotic oscillator

4.1 High Speed Integrated Chaotic Oscillator

Well known LC sinus oscillator is chosen core oscillator to derive a high speed chaos generator. A simple LC resonator can be seen in Figure 4.2.

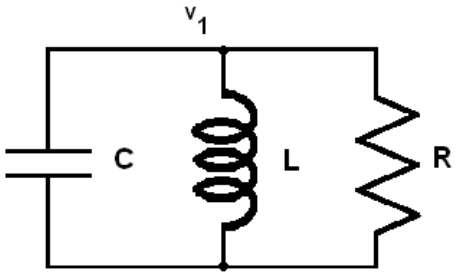

Figure 4.2: LC resonator and tank loss

4.1.1 LC Oscillator

By using Kirchoff's Current Law (KCL) and inductor's current voltage relationship, state equations of the circuit in Figure 4.2 can be derived as follows:

$$C\frac{dV_1}{dt} = -i_L - \frac{V_1}{R} \tag{4.1}$$

$$L\frac{di_L}{dt} = V_1 \tag{4.2}$$

If state variables are rewritten as $x = V_1,\ y = i_L$ and normalize time as $t_n = \frac{t}{\sqrt{LC}}$,

$$dt_n = \frac{dt}{\sqrt{LC}} \tag{4.3}$$

$$\frac{dx}{dt_n} = -\sqrt{\frac{L}{C}}y - \sqrt{\frac{L}{C}}\frac{x}{R} \tag{4.4}$$

$$\frac{dy}{dt_n} = \sqrt{\frac{C}{L}}x \tag{4.5}$$

are obtained. Using relationship $a = \sqrt{\frac{L}{C}}$, state equations are as follows:

$$\dot{x} = -ay - \frac{a}{R}x \tag{4.6}$$

$$\dot{y} = \frac{1}{a}x \tag{4.7}$$

For R=∞, the circuit oscillates sinusoidally as shown in Figure 4.3. The circuit is said to be undamped. The energy that was initially stored in capacitor and inductor can not be dissipated (there are no resistive losses) but simply oscillates back and forth between these two elements. In the absence of damping, this sinusoidal oscillation continues infinitely and the circuit is called a harmonic oscillator.

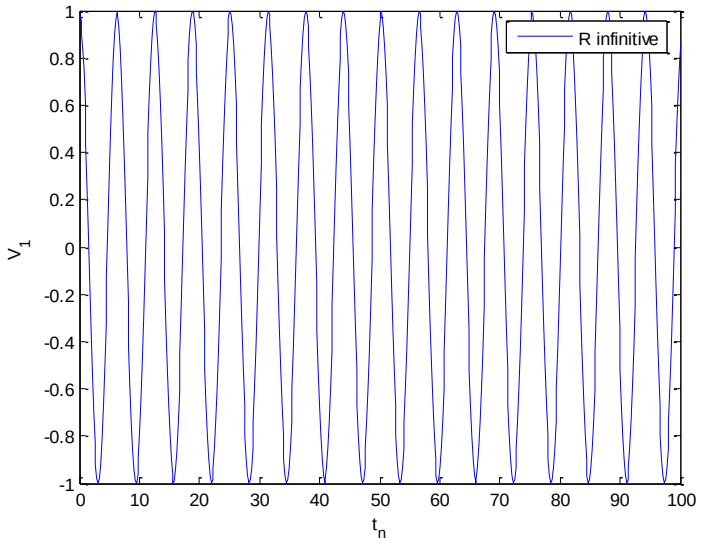

Figure 4.3: Sinusoidal oscillations in LCR resonance circuit in case of R is equal to infinity.

For positive values of R, resonator circuit oscillates damped as shown in Figure 4.4 and energy stored in resonator is dissipated on the resistor to heat.

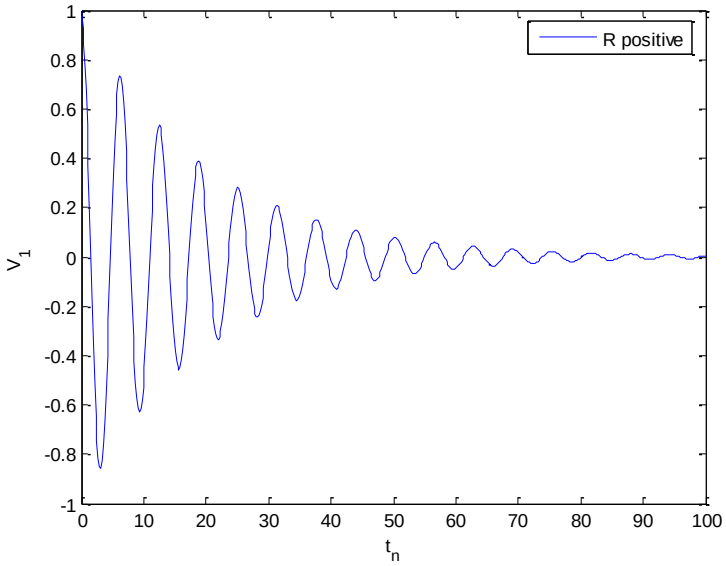

Figure 4.4: For positive values of R, resonator oscillates underdamped.

For negative values of R, the resistor has negative dissipation. It supplies energy to the rest of the circuit. In this case, energy stored in the circuit increases with time. Current and voltages in the circuit have exponentially growing envelopes as shown in Figure 4.5.

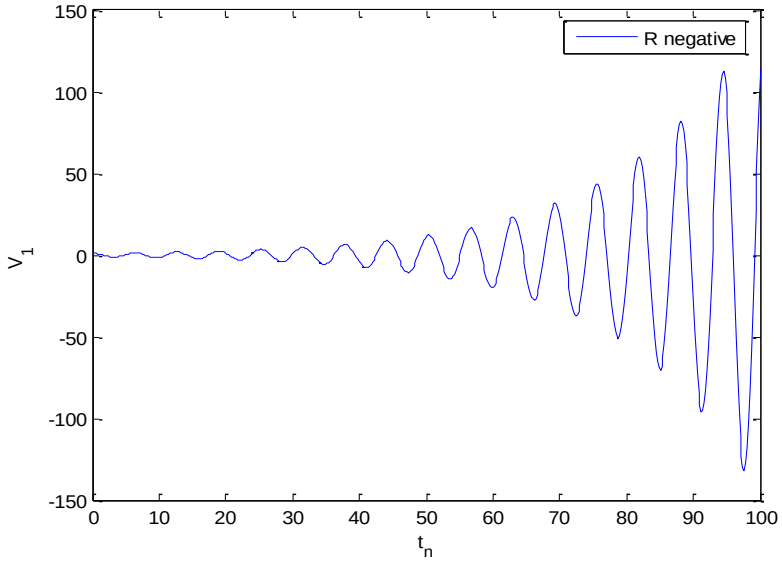

Figure 4.5: Voltage on resonator for negative values of R

A passive only resonator is inadequate for building up oscillation in real world. Energy stored in the resonator is quickly dissipated on the parasitic resistances of inductor and capacitor elements. Active devices such as transistors (biased from DC power supplies) are used to compensate for the loss mechanism on the LC resonant circuit. Then the energy lost in the tank is periodically replenished by the effective negative resistance supplied by the active devices. Such an example of LC oscillator circuit is given in Figure 4.6 and its small signal equivalent circuit is shown in Figure 4.7.

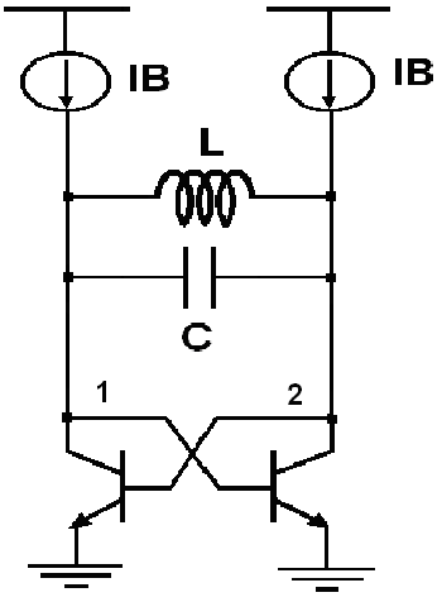

Figure 4.6: Negative-g_m LC sinusoidal oscillator

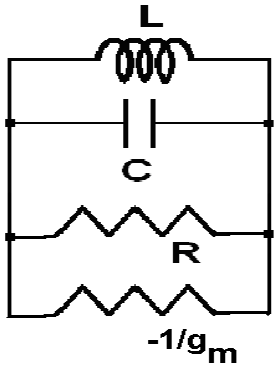

Figure 4.7: Small signal equivalent circuit of negative-g_m LC sinusoidal oscillator

Assuming the oscillator differential (in fact, as a result of nonlinear characteristics of bipolar transistors, oscillator is not fully differential, that is common mode voltage component also varies with time); both terminals of the inductor have common and differential voltage components. If voltage at node 1 is written as $V_C + V_1$ and voltage at node 2 is written as $V_C - V_1$ in Figure 4.6, state equations of the LC oscillator circuit are obtained by using KCL at nodes 1, 2 :

$$2V_1 = L\frac{di_L}{dt} \tag{4.8}$$

$$C\frac{d(2V_1)}{dt} + i_L + I_S e^{\frac{(V_C - V_1)}{V_T}} - I = 0 \tag{4.9}$$

$$-C\frac{d(2V_1)}{dt} - i_L + I_S e^{\frac{(V_C - V_1)}{V_T}} - I = 0 \tag{4.10}$$

Taking difference of (4.9) and (4.10) yields

$$4C\frac{dV_1}{dt} = -2i_L - I_S e^{\frac{V_C}{V_T}}(e^{-\frac{V_1}{V_T}} - e^{\frac{V_1}{V_T}}) \tag{4.11}$$

By adding (4.9) and (4.10), we obtain

$$I_S e^{\frac{V_C}{V_T}}(e^{-\frac{V_1}{V_T}} + e^{\frac{V_1}{V_T}}) = 2I \tag{4.12}$$

$$I_S e^{\frac{V_C}{V_T}} = \frac{2I}{(e^{-\frac{V_1}{V_T}} + e^{\frac{V_1}{V_T}})} \tag{4.13}$$

Rearranging (4.11) by using relationship (4.13) and the tanh definition, we finally obtain following state equations of the LC oscillator circuit:

$$C\frac{dV_1}{dt} = -\frac{1}{2}i_L + \frac{I}{2}\tanh(\frac{V_1}{V_T}) \tag{4.14}$$

$$\frac{di_L}{dt} = \frac{2}{L}V_1 \tag{4.15}$$

By normalizing LC oscillator circuit state equations with

$$\frac{V_1}{V_T} = x \tag{4.16}$$

$$i_L = y \tag{4.17}$$

$$t_n = \frac{t}{\sqrt{LC}} \tag{4.18}$$

$$dt = dt_n\sqrt{LC} \tag{4.19}$$

we obtain the following state equations:

$$\dot{x} = -\frac{1}{2V_T}y + \frac{I}{2V_T}\tanh(x) \tag{4.20}$$

$$\dot{y} = 2V_T x \tag{4.21}$$

By taking bipolar transistors' thermal voltages as V_T=25mV ($V_T = \frac{kT}{q}$,k=Boltzmann constant, T=absolute temperature and q=charge of a single electron) and currents as I=100μA, ordinary differential equations of (4.20) and (4.21) are solved in MATLAB and the graphical solution in Figure 4.8 is obtained.

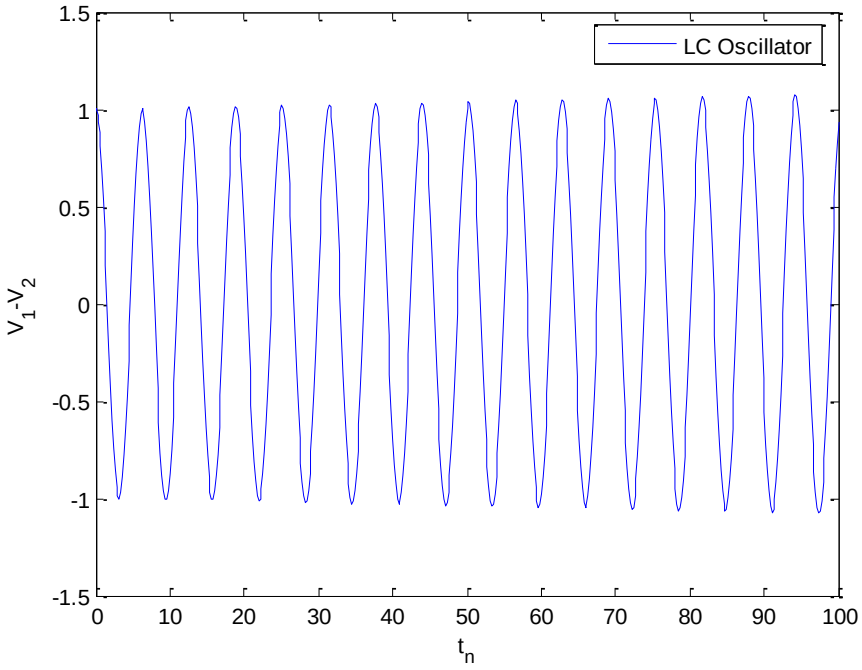

Figure 4.8: Time waveforms obtained from negative-g_m LC sinusoidal oscillator circuit. Y axis is difference of nodes 1 and 2 in Figure 4.6.

4.1.2 Primitive Chaotic Oscillator

In order to exhibit chaos electronically, an autonomous circuit consisting of resistors, capacitors, and inductors must contain

1. at least one nonlinear element
2. at least one negative resistor
3. at least three energy-storage elements such as capacitors, inductors or mixing two of them.

We add another RC network, a negative resistor and a nonlinear element to the simple LC resonator circuit to build the chaotic oscillator as shown in Figure 4.9. The nonlinear element in this circuit is a transconductance element implementing the signum function.

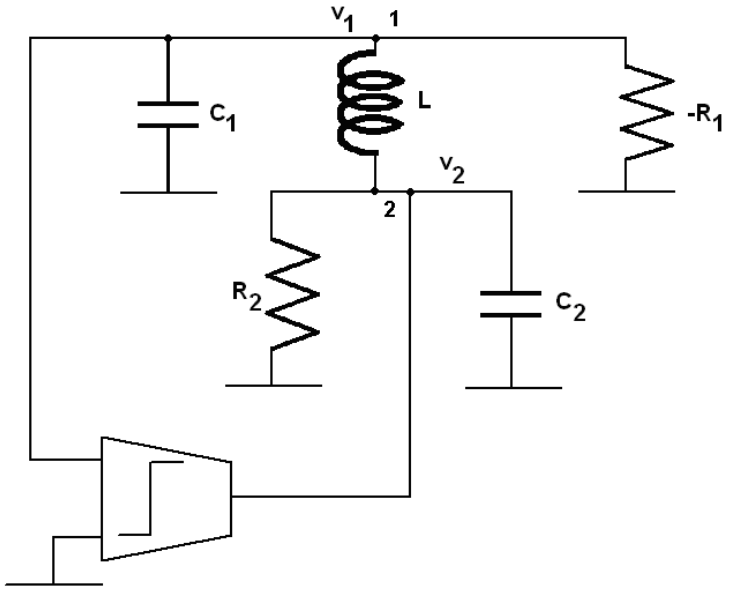

Figure 4.9: Primitive chaotic oscillator

State equations of this circuit is obtained as follows:

By using KCL at node 1, equation (4.22) is obtained.

$$C_1 \frac{dV_1}{dt} = -i_L + \frac{V_1}{R_1} \tag{4.22}$$

KCL at node 2 and inductor's current voltage relationship yield the following equations:

$$C_2 \frac{dV_2}{dt} = \text{sgn}(V_1) + i_L - \frac{V_2}{R_2} \tag{4.23}$$

$$V_1 - V_2 = L \frac{di_L}{dt} \tag{4.24}$$

Changing state variables as $V_1 = x$, $Ri_L = y$, $V_2 = z$, taking $C = C_1 = C_2$ and normalizing time as $t_n = \frac{t}{RC}$ in (4.22) - (4.24), we conclude with the following simplified state equations:

$$\dot{x} = -y + \frac{R}{R_1} x \tag{4.25}$$

$$\dot{x} = R\,\mathrm{sgn}(x) + y - \frac{R}{R_2} z \tag{4.26}$$

$$\dot{y} = \frac{R^2}{\left(\frac{L}{C}\right)} (x - z) \tag{4.27}$$

State equations derived above were analyzed with MATLAB tool. For the following parameter values, the circuit exhibits a double-scroll chaos oscillator behavior:

$$\frac{R^2}{\left(\frac{L}{C}\right)} = 1 \tag{4.28}$$

$$\frac{R}{R_1} = 0.6 \tag{4.29}$$

$$\frac{R}{R_2} = 2 \tag{4.30}$$

Solutions of state equations (4.25) – (4.27) in time domain are given in Figure 4.10.

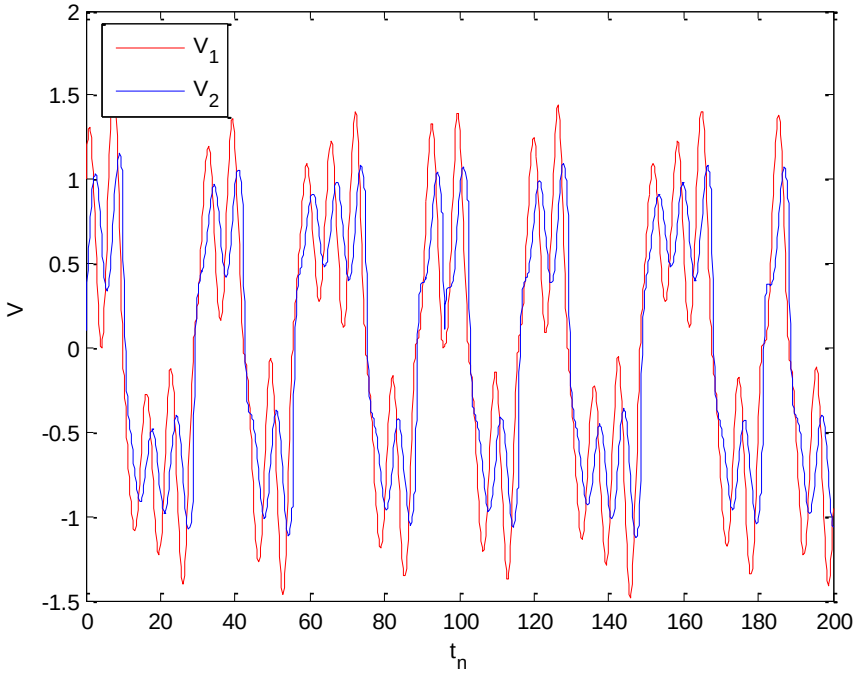

Figure 4.10: Chaos Oscillator node voltages waveform

X-Z plane trajectory of the circuit is given in Figure 4.11.

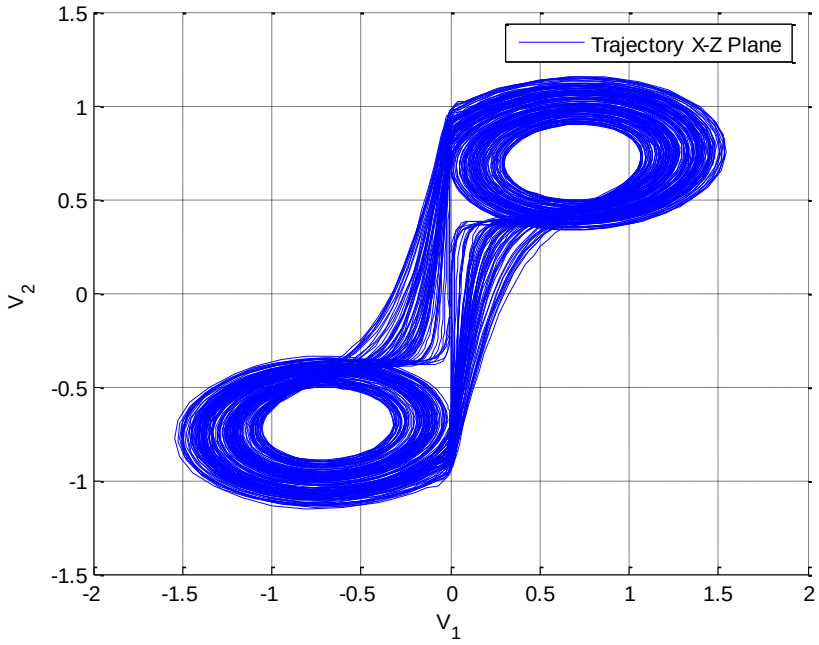

Figure 4.11: X-Z plane trajectory obtained from numerical simulations.

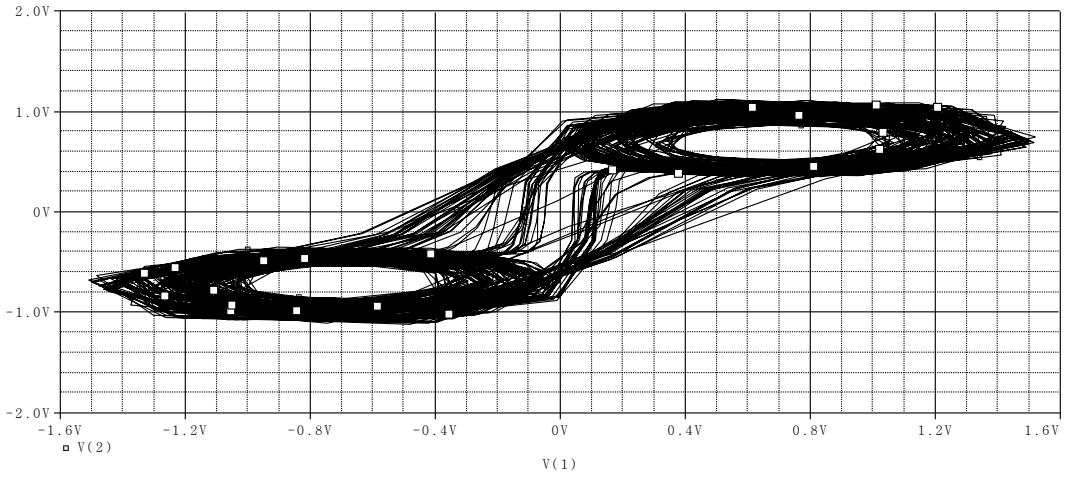

Figure 4.12: X-Z plane obtained trajectory from SPICE simulations. X axis is the voltage at node 1 and Y axis is the voltage at node 2 in Figure 4.9.

X-Y-Z plane trajectory of the circuit is given in Figure 4.13.

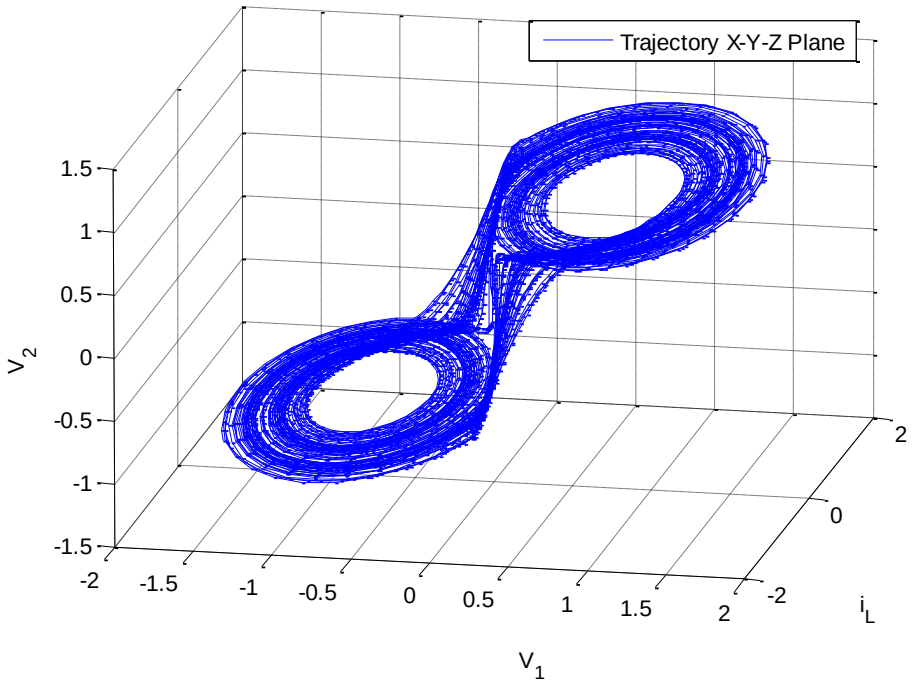

Figure 4.13: X-Y-Z plane trajectory obtained from numerical simulations

4.1.3 High Speed Integrated Chaotic Oscillator

Chaotic oscillator derived from the structure in Figure 4.9 is given in Figure 4.14.

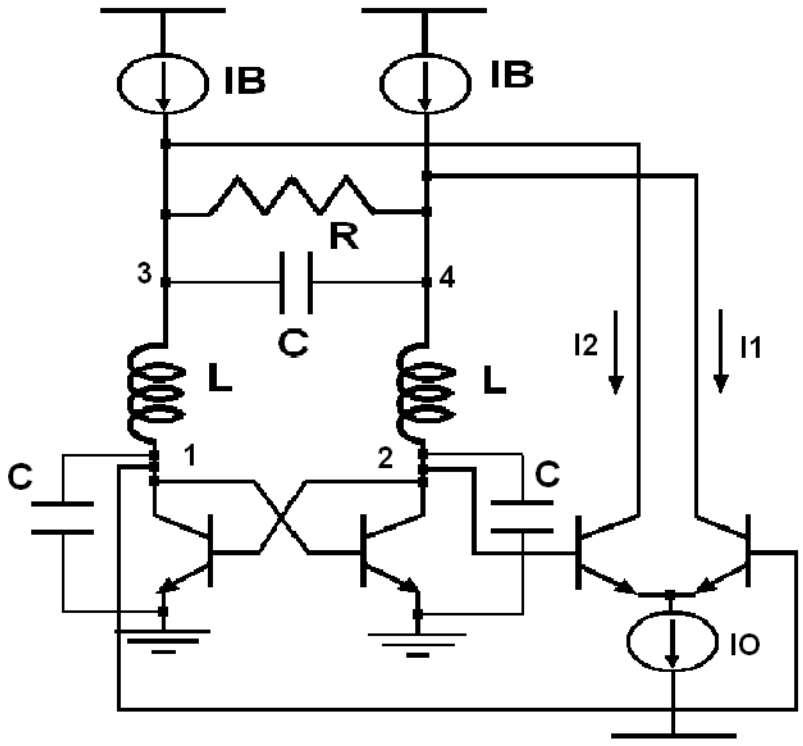

Figure 4.14: High speed integrated chaotic oscillator

State equations of chaotic oscillator circuit in Figure 4.14 are derived as follows;

We take node voltages in Figure 4.14 as:

1. Voltage at node 1 is $V_C + V_1$, at node 2 is $V_C - V_1$, at node 3 is $V_C + V_2$ and at node 4 is $V_C - V_2$ (where V_C is half of the sum of node voltages 1, 2 and also 3, 4; V_1 is half of the difference of node voltages 1, 2 and V_2 is the half of the difference of node voltages 3, 4),
2. Current of inductance on the left side is $I_L - i_L$, on the right side is $I_L + i_L$.

V_T and I_S are the thermal voltage and bipolar transistor reverse saturation current, respectively. I_B and I_O are DC bias currents.

Using KCL at node 1, we obtain

$$C\frac{d(V_C + V_1)}{dt} + I_S e^{\frac{V_C - V_1}{V_T}} - I_L + i_L = 0 \tag{4.31}$$

Using KCL at node 2, we obtain

$$C\frac{d(V_C - V_1)}{dt} + I_S e^{\frac{V_C + V_1}{V_T}} - I_L - i_L = 0 \tag{4.32}$$

Using KCL at node 3, we obtain

$$I_L - i_L + I_2 + \frac{2V_2}{R} + C\frac{d(2V_2)}{dt} - I_B = 0 \tag{4.33}$$

Using KCL at node 4, we obtain

$$I_L + i_L + I_1 - \frac{2V_2}{R} - C\frac{d(2V_2)}{dt} - I_B = 0 \tag{4.34}$$

If we subtract equation (4.32) from (4.31) we conclude with

$$C\frac{dV_1}{dt} = -i_L + \frac{I_S e^{\frac{V_C}{V_T}}}{2}\left(e^{\frac{V_1}{V_T}} - e^{-\frac{V_1}{V_T}}\right) \tag{4.35}$$

If we subtract equation (4.34) from (4.33) we conclude with

$$C\frac{dV_2}{dt} = -\frac{V_2}{R} + \frac{i_L}{2} + \frac{I_1 - I_2}{4} \tag{4.36}$$

Using bipolar differential pair's output current-input differential voltage relationship and equation (4.36), we derive

$$C\frac{dV_2}{dt} = -\frac{V_2}{R} + \frac{i_L}{2} + \frac{I_O}{4}\tanh\left(\frac{V_1}{V_T}\right) \tag{4.37}$$

If we add equation (4.31) and (4.32) we conclude with

$$C\frac{dV_C}{dt} = I_L - \frac{I_S e^{\frac{V_C}{V_T}}}{2}\left(e^{\frac{V_1}{V_T}} + e^{-\frac{V_1}{V_T}}\right) \tag{4.38}$$

Using inductor voltage-current relationship we obtain

$$\left(V_C + V_2\right) - \left(V_C + V_1\right) = L\frac{d(I_L - i_L)}{dt} \tag{4.39}$$

$$V_1 - V_2 = L\frac{d(i_L)}{dt} \tag{4.40}$$

Equations (4.35), (4.37), (4.38) and (4.40) are state equations of the circuit in Figure 4.14. For the sake of simplicity, we use the following normalized quantities in which V_S is an arbitrary scaling voltage,

$$x = \frac{V_1}{V_S} \tag{4.41a}$$

$$y = \frac{i_L R}{V_S} \tag{4.41b}$$

$$z = \frac{V_2}{V_S} \tag{4.41c}$$

$$x_C = \frac{V_C}{V_S} \tag{4.41d}$$

$$R = \sqrt{\frac{L}{C}} \tag{4.41e}$$

$$a = \frac{V_S}{V_T} \tag{4.41f}$$

$$t = \frac{t_n}{RC} \tag{4.41g}$$

The above system of equations is transformed into the following dimensionless system of ordinary differential equations:

$$\dot{x} = -y + \frac{c_S e^{ax_C}}{2}\left(e^{ax} - e^{-ax}\right) \tag{4.42}$$

$$\dot{y} = x - z \tag{4.43}$$

$$\dot{z} = -z + \frac{y}{2} + \frac{c_O}{4}\tanh(ax) \tag{4.44}$$

$$\dot{x}_C = c_B - \frac{c_S e^{ax_C}}{2}\left(e^{ax} + e^{-ax}\right) \tag{4.45}$$

where $c_S = \frac{I_S R}{aV_T}$, $c_O = \frac{I_O R}{aV_T}$ and $c_B = \frac{(I_B - \frac{I_O}{2})R}{aV_T}$.

The equations (4.42) – (4.45) can generate chaos for several sets of parameters. For example, the chaotic attractor shown in Figure 4.15 is obtained from numerical analysis of the system with parameters a=0.5, C_B= 2, C_S=10^{-4} and C_O=8.8, by using Dormand-Prince numerical integration method [11].

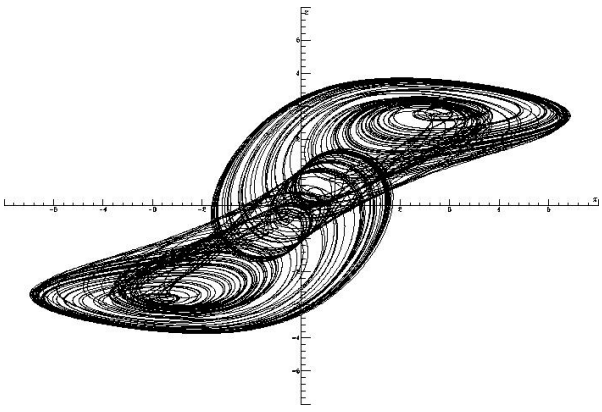

Figure 4.15: Results of numerical analysis of the system in Figure 4.14.X axis is the state variable x and Y axis is the state variable y.

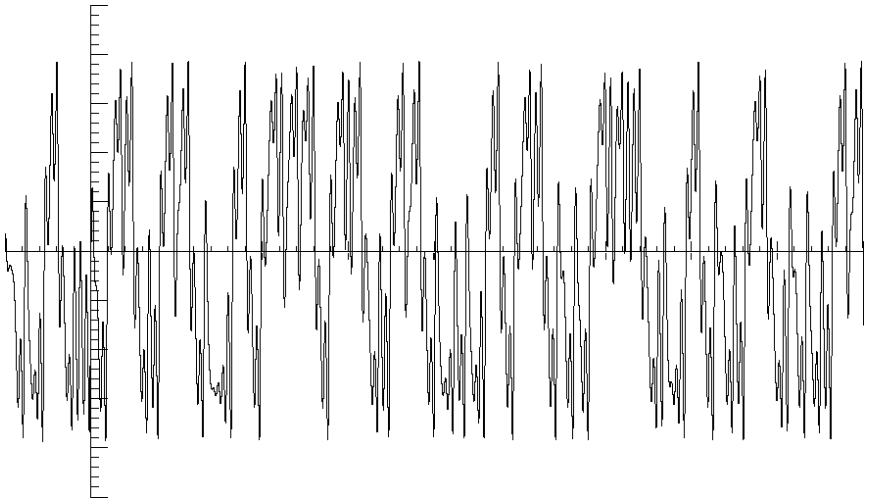

Figure 4.16: Time domain waveform of x variable obtained from numerical analysis of the system in Figure 4.14.

4.2 Random Bit Generator

To obtain binary random bits from the chaotic attractor, method in [1] is used. The state-space of the chaotic attractor is partitioned into three subspaces, V_0, V_{tr} and V_1 determined by the planes $x=c_0$ and $x=c_1$, shown in Figure 4.17. A bit 1 is generated when the trajectory passes from the region V_{tr} to region V_1 and a bit 0 is generated when the trajectory passes to region V_0 from region V_{tr}.

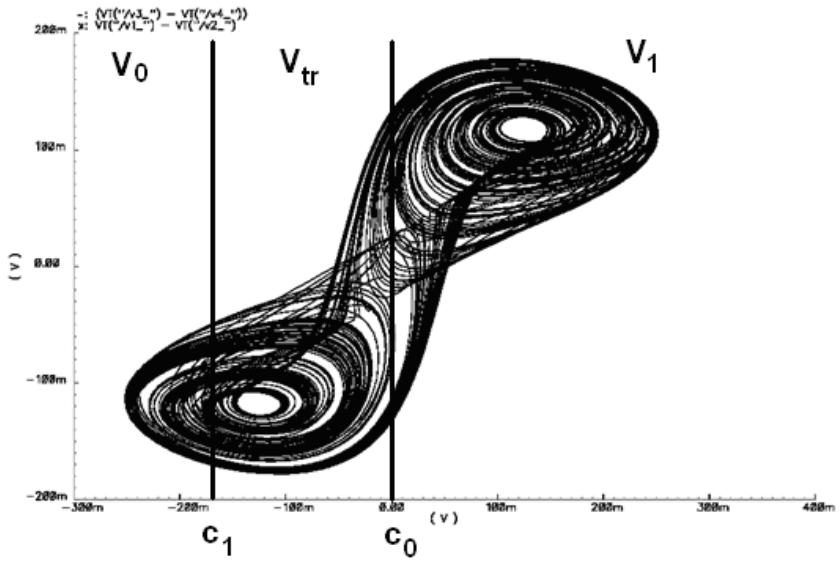

Figure 4.17: Partitioned subspaces of chaotic attractor

In order to remove bias in this sequence and improve statistical properties of generated bit streams, the well known Von Neumann's de-skewing technique is employed. Overall system block diagram is shown in Figure 4.18.

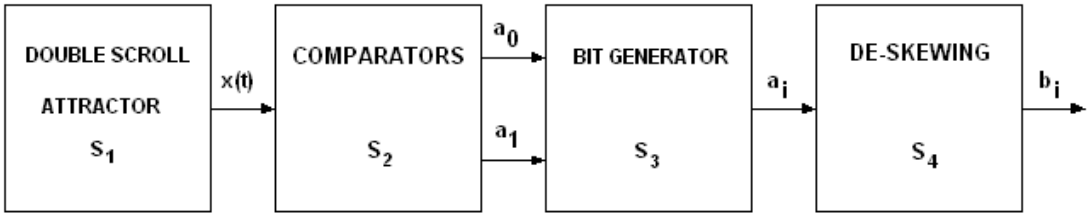

Figure 4.18: Random bit generation from chaotic oscillator block diagram

4.2.1 Comparator

Chaotic voltage signal at node 2 is subtracted from the voltage signal at node 1 in Figure 4.14 and resulting difference voltage is sampled according to the method described above to generate random bits. The resulting voltage signal difference expresses the state variable x of the system of state equations described in section 4.1.3. Thresholds c_0 and c_1 is illustrated in Figure 4.19 with time domain waveform of the chaotic signal x(t).

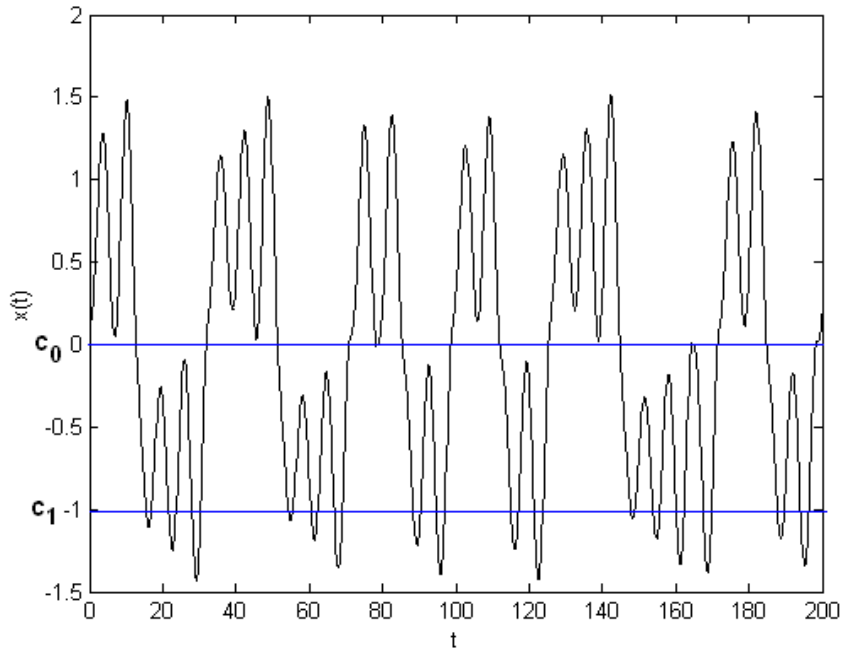

Figure 4.19: Thresholds c_0 and c_1

Two threshold functions are realized with comparators as shown in Figure 4.20 by taking $c_0 = 0$ and c_1 as a variable threshold.

4.2.2 Bit Generator

Logical OR operation is performed at outputs of two comparator circuits to generate a clock signal as shown in Figure 4.21. This clock signal identifies that a certain bit either a 1 or a 0 is generated. A D type flip-flop circuit is clocked with the generated clock signal. D input of the flip-flop circuit is directly taken from the first comparator's output a_0 since when a bit 1 is generated, first comparator output is 1 and vice versa. Bit generator block is given in Figure 4.21.

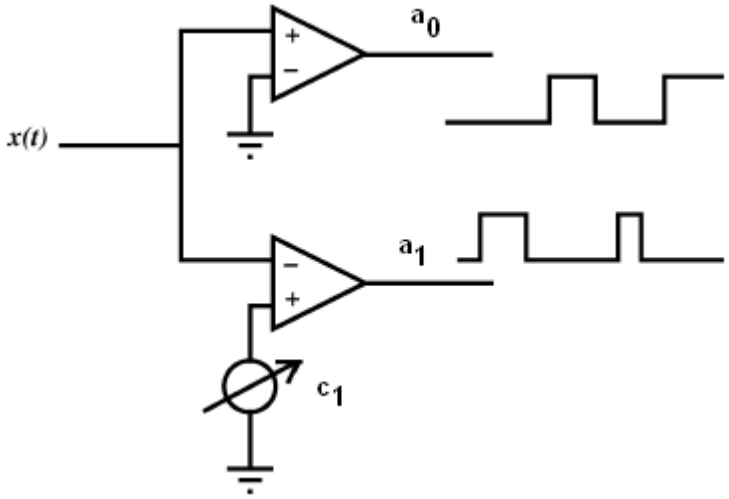

Figure 4.20: Comparator circuits to generate bits

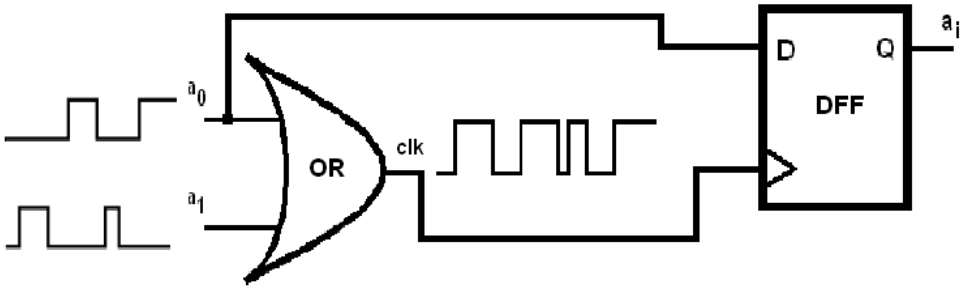

Figure 4.21: Bit generator block

In order to guarantee correct operation of above circuit, OR gate propagation delay should be slightly higher than setup time of the D-type flip-flop circuit.

$$t_{P(OR)} \geq t_{setup(DFF)} \tag{4.46}$$

4.2.3 De-Skewing

A natural source of random bits may not supply unbiased bits as a direct output. De-skewing techniques are to extract unbiased bits from a defective generator with unknown bias. These techniques also eliminate the correlations in the output of the natural sources of random bits. Von-Neumann's de-skewing process converts nonoverlapping pairs of bits into output bits by converting the bit pair 0 1 into an output 0, converting 1 0 into an output 1. The pairs 1 1 and 0 0 are discarded. Logic-level diagram of Von-Neumann's de-skewing method is shown in Figure 4.22. Clock signal generated by the comparators is divided by 2 in order to lookup nonoverlapping bit pairs. For each nonoverlapping bit pairs, if the exor operation results 0, divided clock is disabled by the "and" gate. If the result is 1, then the "and" gate output is as same as the divided clock output. Thus, 0 1 and 1 0 bit pairs are successfully translated to a bit 0 or 1, respectively. System timing diagram is shown in Figure 4.23.

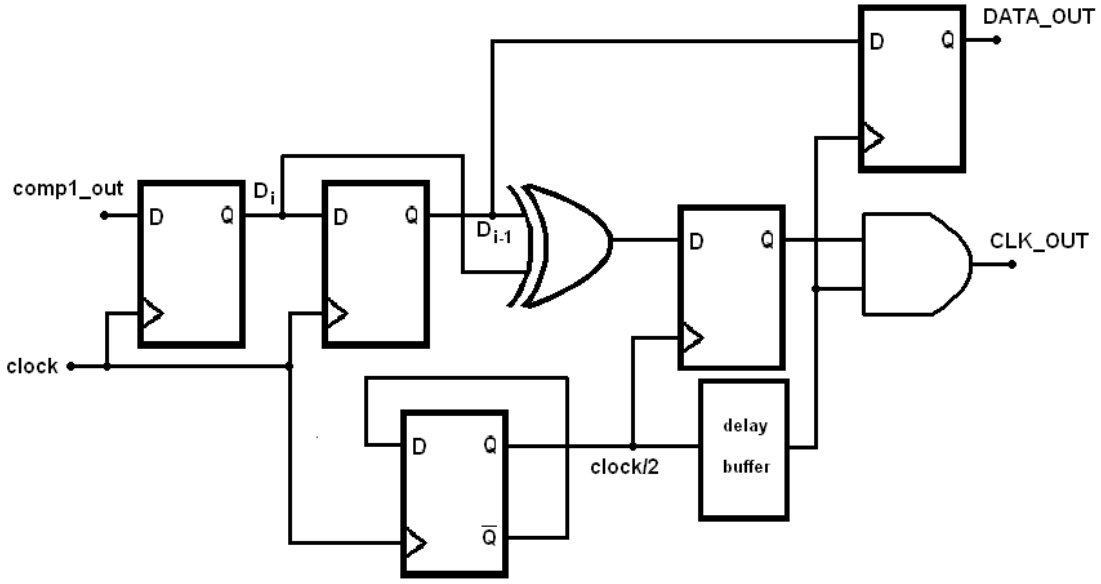

Figure 4.22: De-Skewing block

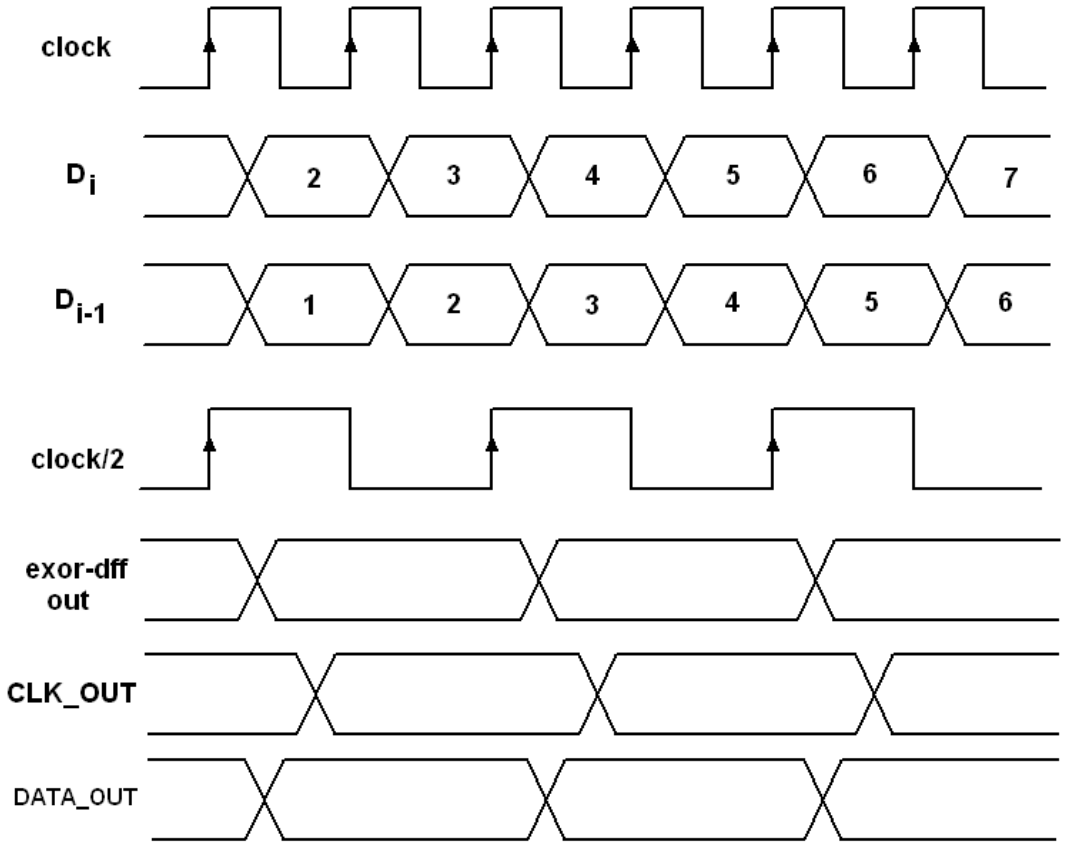

Figure 4.23: De-skewing system timing diagram

5. CIRCUIT LEVEL DESIGN

The chaotic circuit was designed and simulated both in AustriaMikroSytems 0.35 µm SiGe BiCMOS (f_{Tmax} = 70 GHz) and IHP 0.25 µm SiGeC BiCMOS (f_{Tmax} = 80 GHz) technologies. The whole system was designed using IHP 0.25 µm SiGeC BiCMOS technology. Highest transit frequency of the high speed npn bipolar devices in this technology is 80GHz with a collector-emitter breakdown voltage of 2.4 V. IHP's 0.25µm SiGeC BiCMOS process also includes standard (f_T=50GHz, V_{CEBO}=4V) and high voltage (f_T=30GHz, V_{CEBO}=7V) bipolar transistors, high-Q MIM (Metal Insulator Metal) capacitor, salicided and unsalicided polysilicon resistors, 4-layer Al interconnect metal and 2µm thick fourth layer metal to realize high-Q inductors. Cadence Spectre® circuit simulator was used during simulations. The supply voltages are ±1.2V for V_{CC} and V_{EE}, respectively.

5.1 Chaotic Circuit

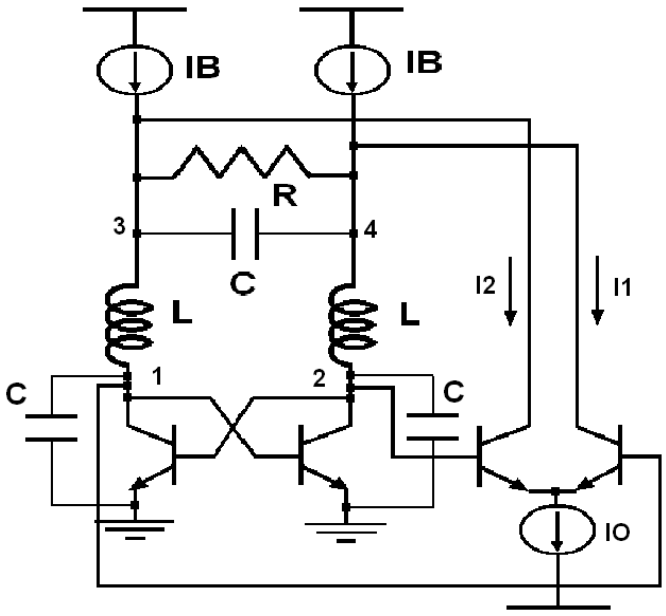

Figure 5.1: Chaotic circuit

The chaotic oscillator in Figure 5.1 was numerically simulated and verified to generate chaos with parameters, a=0.5, C_B= 2, C_S=10^{-4} and C_0=8.8 in section 4.1.3 . These parameters are related to the circuit design variables below:

$$c_S = \frac{I_S R}{a V_T} \tag{4.47}$$

$$c_O = \frac{I_O R}{a V_T} \tag{4.48}$$

$$c_B = \frac{(I_B - \frac{I_O}{2})R}{a V_T} \tag{4.49}$$

Using parameter equations (4.47) – (4.49) and taking L=11.7nH (which is a standard inductance value available in the used technology), C=350fF and $R = \sqrt{\frac{L}{C}} = 182\Omega$, I_O and I_B currents are found to be 600μA and 710μA, respectively. Due to nonidealities that were not concerned during deriving the state equations of circuit in Figure 5.1, such as inductance series resistance, parasitic bipolar transistor terminal resistances and bipolar transistor operation in saturation region, circuit does not exhibit chaos with the current values above. During Spectre simulations, I_B current was taken 800μA to generate chaos. Also large bipolar transistors were used for the cross-coupled pair to reduce the parasitic terminal resistances, especially the base terminal resistance. Inductance's and bipolar transistors' parasitic terminal capacitance values were subtracted from the C value in the circuit. PMOS current mirror transistors with aspect ratio of 100μm/0.8μm were used to realize I_B current sources. Spectre simulation results of the circuit in Figure 5.1 are given in Figures 5.2 and 5.3.

5.2 Integrated Analog Tunable Resistor

The high-speed chaotic oscillator described in section 5.1 was simulated with several process and temperature variations with Spectre. Temperature was swept from -20^0C

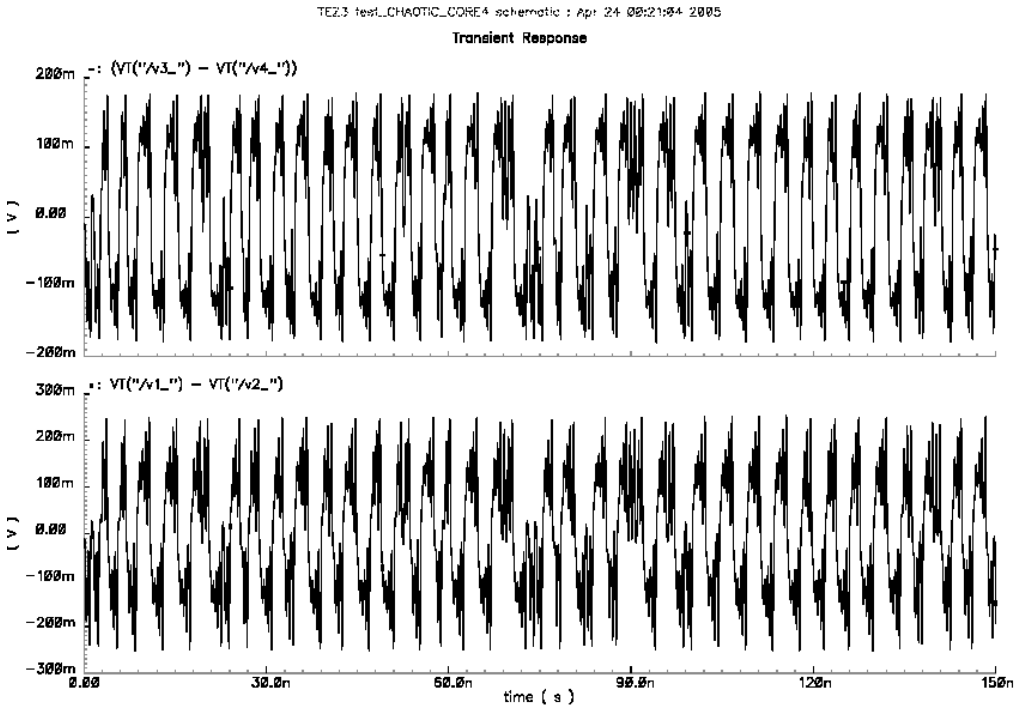

Figure 5.2: Chaotic transient waveforms from Cadence simulation of the high frequency circuit.

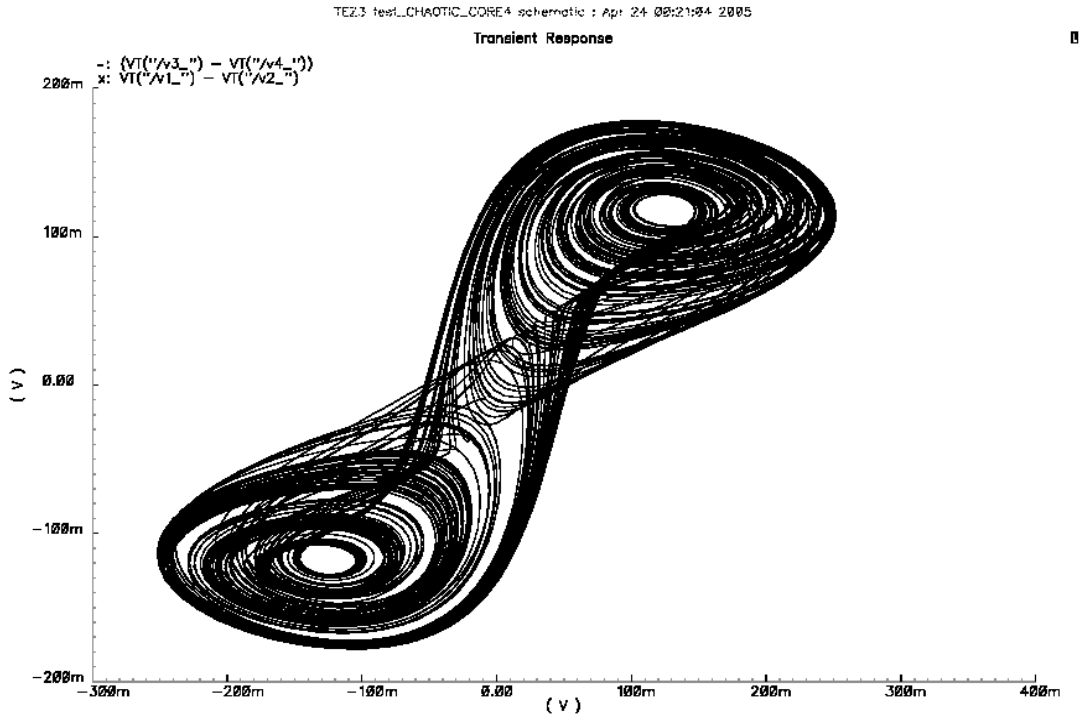

Figure 5.3: Chaotic attractor from Cadence simulation of the high frequency circuit.

to 50^0C and it is observed that chaotic oscillator is functional along this temperature range.

Bipolar transistor current gain, transit frequency and reverse saturation current variations in the used BiCMOS process do not affect functionality of the circuit, too. MIM (Metal Insulator Metal) capacitor's and polysilicon resistor's relative deviations are %10 and %25 in used BiCMOS process, respectively. With Spectre simulations, it was observed that %10 variations of capacitances are tolerable for functionality of the chaotic oscillator, however for the polysilicon resistor this is not the case. We can only tolerate %10 changes of the resistor value in the chaotic oscillator for achieving chaotic operation, which is below %25 nominal process value. It is concluded that a tunable resistance structure should be used to tolerate process variations.

A PMOS transistor can be used to realize an on-chip tunable resistor. On resistance of a MOS transistor operating in deep triode region can be approximated from the triode I-V relationship as given below:

$$R_{ON} = \frac{1}{\mu_n C_{ox} \frac{W}{L}(V_{GS} - V_{TH})} \tag{4.50}$$

Therefore a MOSFET can operate as a resistor whose value is controlled by its overdrive voltage, as long as the transistor is operating with small $|V_{DS}|$ values [12]. A regulation circuit must be designed in order to apply the correct gate source voltage to the device to obtain the required resistor value. Disadvantages of a PMOS resistor are parasitic capacitances of its terminals and its non-linear I-V characteristic for relatively larger values of its $|V_{DS}|$ voltage. In contrast, on-chip polysilicon resistors have good linearity and low parasitic capacitances thanks to the thick poly-substrate oxide. The approach used in this work to realize an integrated tunable resistor is to combine the advantages of both PMOS and polysilicon resistors. Both devices are connected as shown in Figure 5.4 [13].

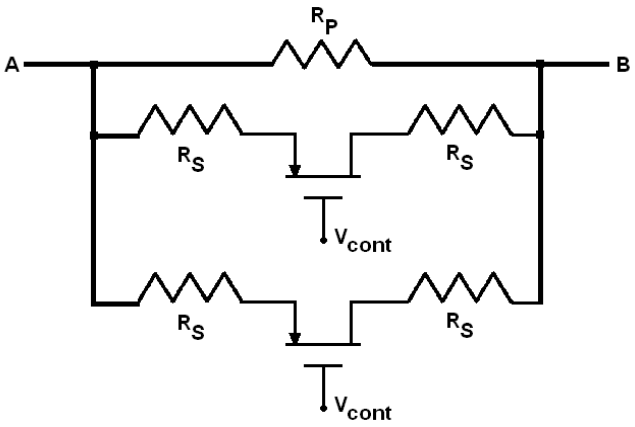

Figure 5.4: Integrated tunable resistor

In Figure 5.4, R_P resistance drives much of the current in order to decrease PMOS current. Resistances R_S reduce source-drain voltage difference of PMOS resistor for better linearity [14]. Parallelizing two identical PMOS-resistor structures gives ability to use higher R_S resistance and smaller PMOS transistor to provide better linearity. Resistance between A and B terminals can be controlled via applied PMOS transistor's gate voltage. Polysilicon resistance R_P is equal to 225Ω, which is +25% higher than nominal value of the resistance 180Ω. For best-case process corner, resistance value deviates relatively by -25%, PMOS gate voltage is equal to V_{DD} and it is OFF. In this case, target value of the resistance is achieved. For typical and worst case conditions, PMOS transistor is ON and contributes to a resistance between A and B terminals equal to 180Ω with help of the impedance regulation circuit shown in Figure 5.5.

R_{EXT1} and R_{EXT2} are off-chip resistor components. Analog impedance regulation works as follows: A replica of integrated tunable resistor structure is placed between two externally connected resistors R_{EXT1} and R_{EXT2}, respectively. R_{EXT2} off-chip resistor value is higher than R_{EXT1} resistor value by one reference resistance value. Negative feedback in the circuit forces two inputs of the opamp circuit to be equal. Therefore, tunable resistor value is equal to (R_{EXT2}-R_{EXT1}) which is set to desired on-chip resistance value. V_{ref} voltage is set to $\frac{VDD}{2}$. By using this impedance regulation circuit, the needed V_{cont} voltage is generated and can be applied to the main structure. On-chip polysilicon resistances R_P and R_S are equal to 450Ω and 100Ω, respectively. PMOS transistors' aspect ratio is 20μm/0.25 μm. Integrated tunable resistance is simulated with Spectre in typical process corner ($T=27^0C$), best-case process corner ($T=-20^0C$) and worst-case process corner ($T=50^0C$) and the simulation results of the DC resistance of topology is shown in Figure 5.6. A CMOS Miller-OTA is used in the impedance regulation circuit as the amplifier.

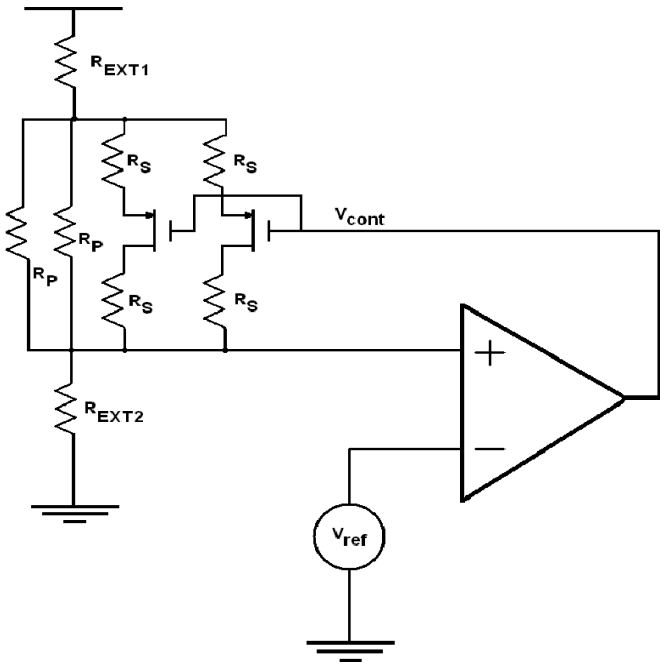

Figure 5.5: Impedance regulation circuit

Integrated tunable resistor was simulated with the chaotic circuit to tolerate resistance variations of process. The chaotic attractor obtained from simulation of the chaotic oscillator for the worst-case process corner is shown in Figure 5.7. It is worth to note here that there is still nonlinearity in the tunable resistance circuit because of PMOS transistor's nonlinear characteristic.

5.3 Difference Amplifier Circuit

Difference of terminal voltages 1 and 2 in circuit shown in Figure 5.1 is sampled to generate random bits in the used random bit generator topology. Resistor degenerated differential pair amplifier is used for difference operation to provide linearity to perform open loop difference operation. For the reason that chaotic oscillator is operating at high speed and opamps have limited gain-bandwidth products for stability issues, closed-loop difference amplifier topology is not chosen.

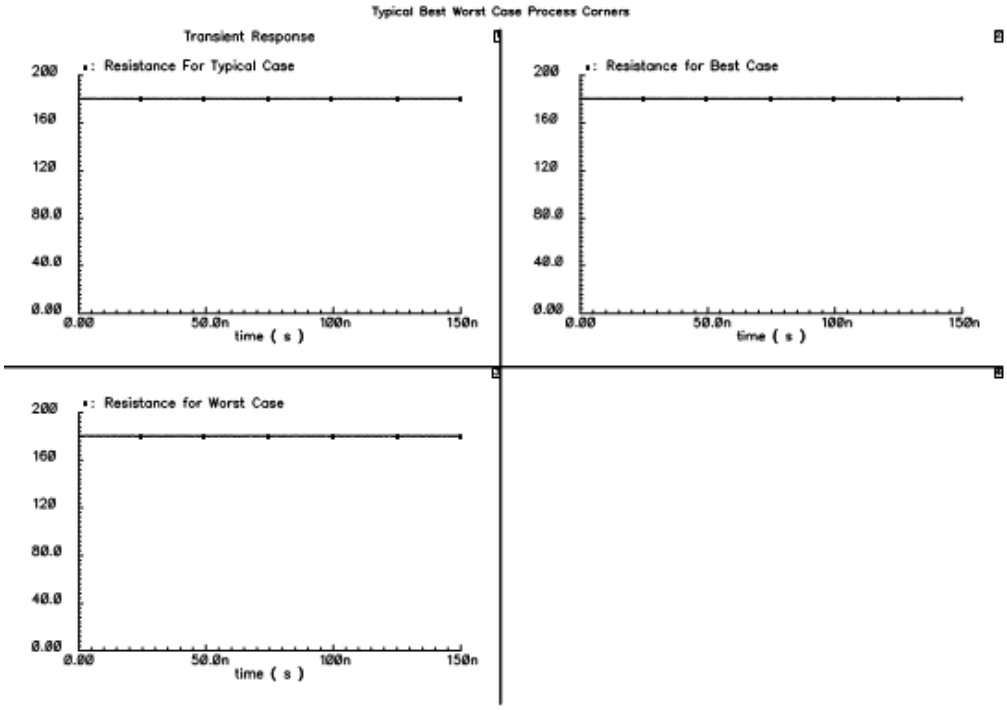

Figure 5.6: DC resistance of integrated tunable resistor in typical-, best- and worst-case process corners

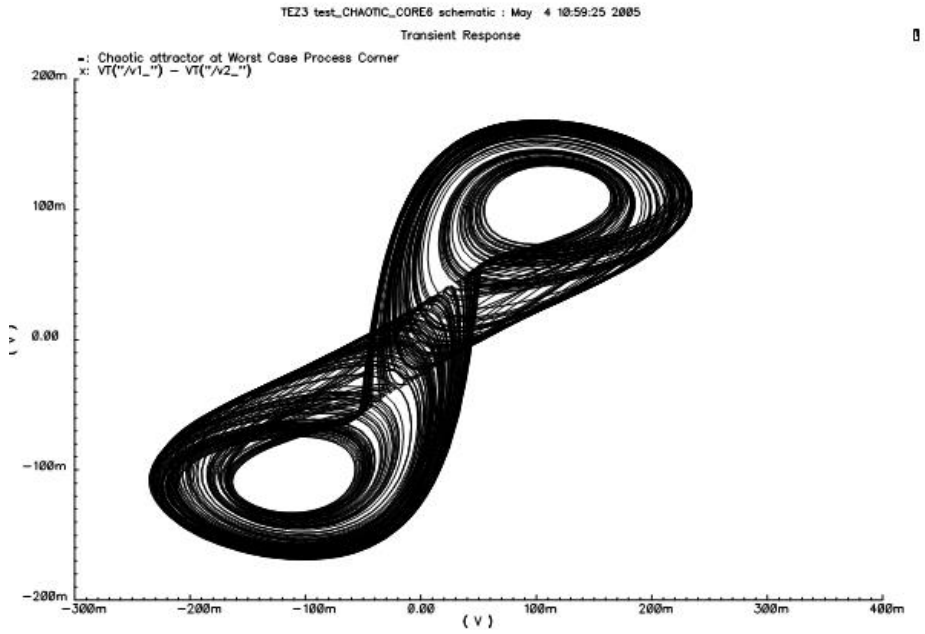

Figure 5.7: Chaotic attractor obtained from Spectre simulations of chaotic oscillator with integrated tunable resistor in worst case process corner.

The open-loop difference amplifier circuit schematic is given in Figure 5.8. R is equal to 600Ω and all bipolar transistors' emitter currents are 500μA in the circuit.

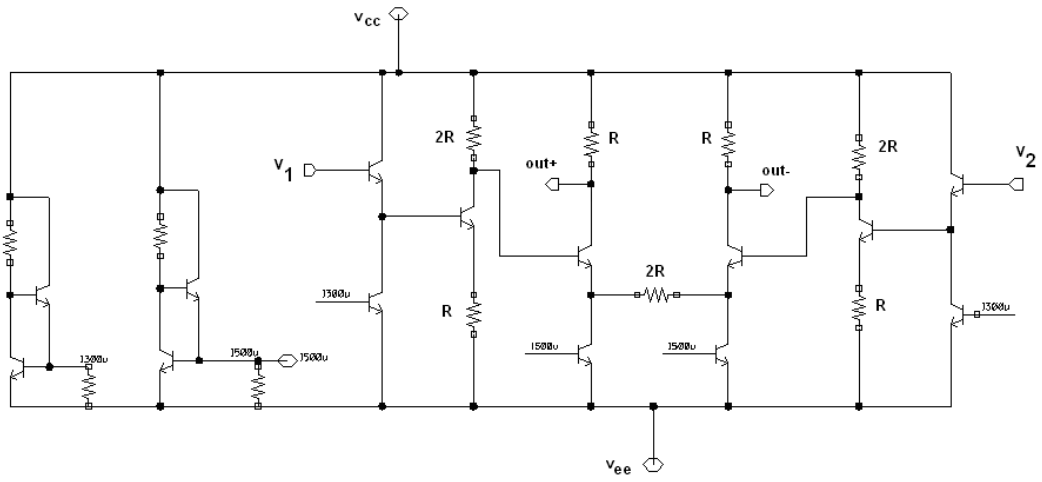

Figure 5.8: Difference amplifier circuit

Spectre simulation results are given in Figure 5.9. Above two waveforms are input and below two waveforms are negative and positive output voltages of the circuit. Ideal differences of inputs voltages are also shown. From Figure 5.9, it is seen that circuit is taking difference of two waveforms successfully by using degeneration.

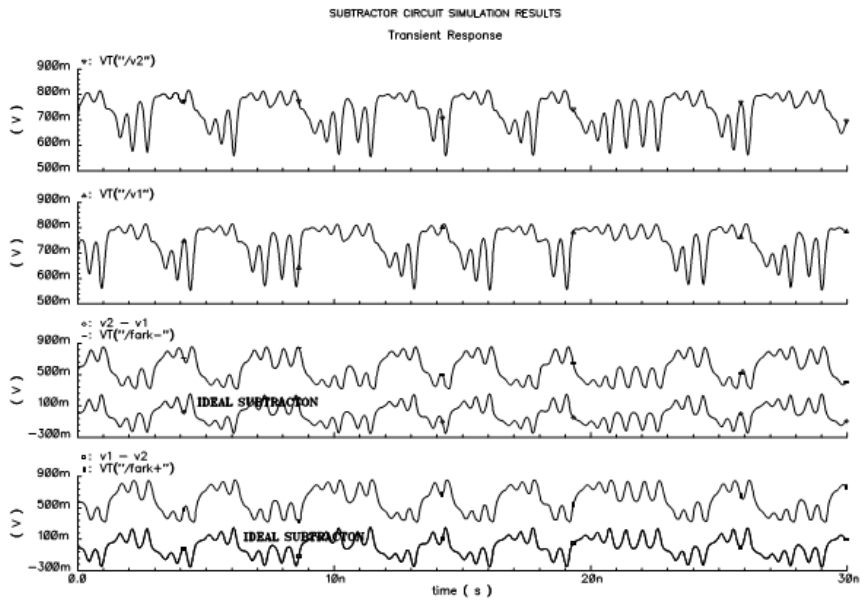

Figure 5.9: Difference amplifier circuit simulation results

5.4 Comparator Circuit

The comparator circuit schematic is shown in Figure 5.10. Since comparators used in the system are asynchronous, latch type comparator topologies with positive feedback were not used. The comparator circuit is a high-gain 3-stage amplifier. The voltage difference between the input and the reference is amplified to logic levels in the circuit by this high gain. Resistance values are 700Ω and each differential pair's tail current is 300μA.

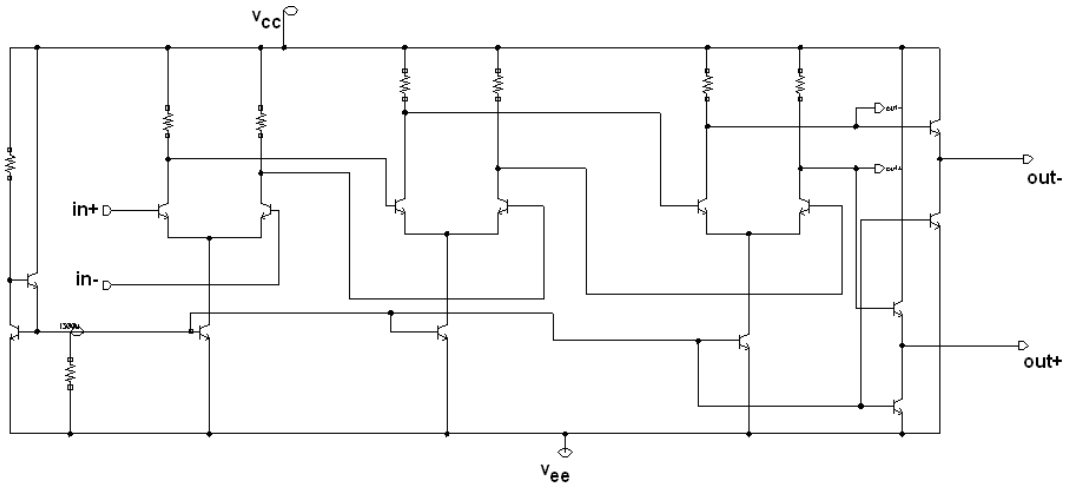

Figure 5.10: Comparator Circuit

Comparator circuit simulation results are shown in Figures 5.11-12. As seen in Figures, when comparator input voltage is above its reference voltage, output of the comparator become logic high and , when comparator input voltage is below its reference voltage, output of the comparator become logic low with an input output delay of 80ps.

5.5 Or Gate

The OR gate used in the system is a standard ECL type bipolar logic gate. Its schematic is shown in Figure 5.13. Differential pair's tail current is 1mA and collector resistances are 300Ω in the circuit. OR gate generated clock signal drives 3 DFFs. In order to improve driving strength of the OR gate, emitter follower tail currents were chosen 2mA.

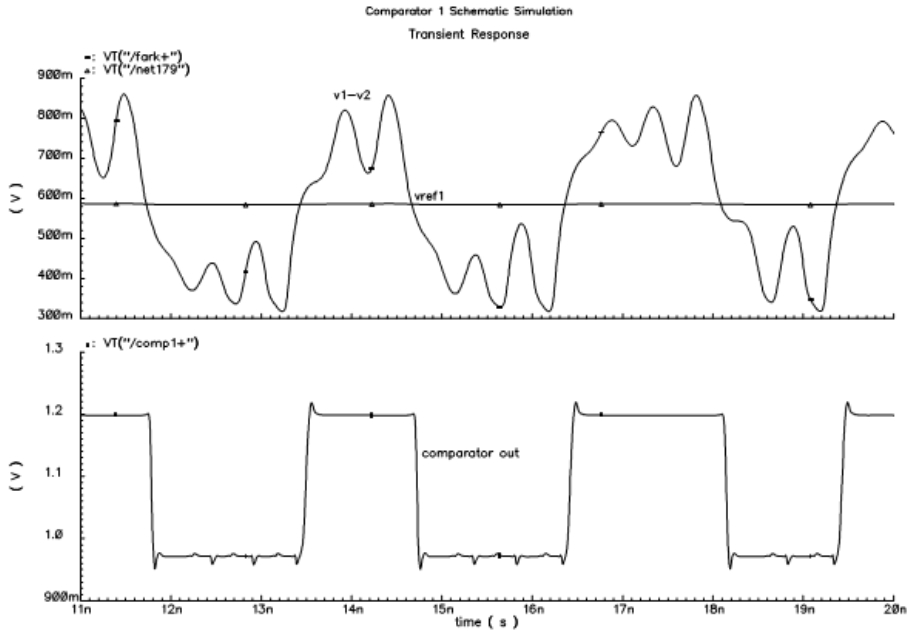

Figure 5.11: First comparator circuit simulation results

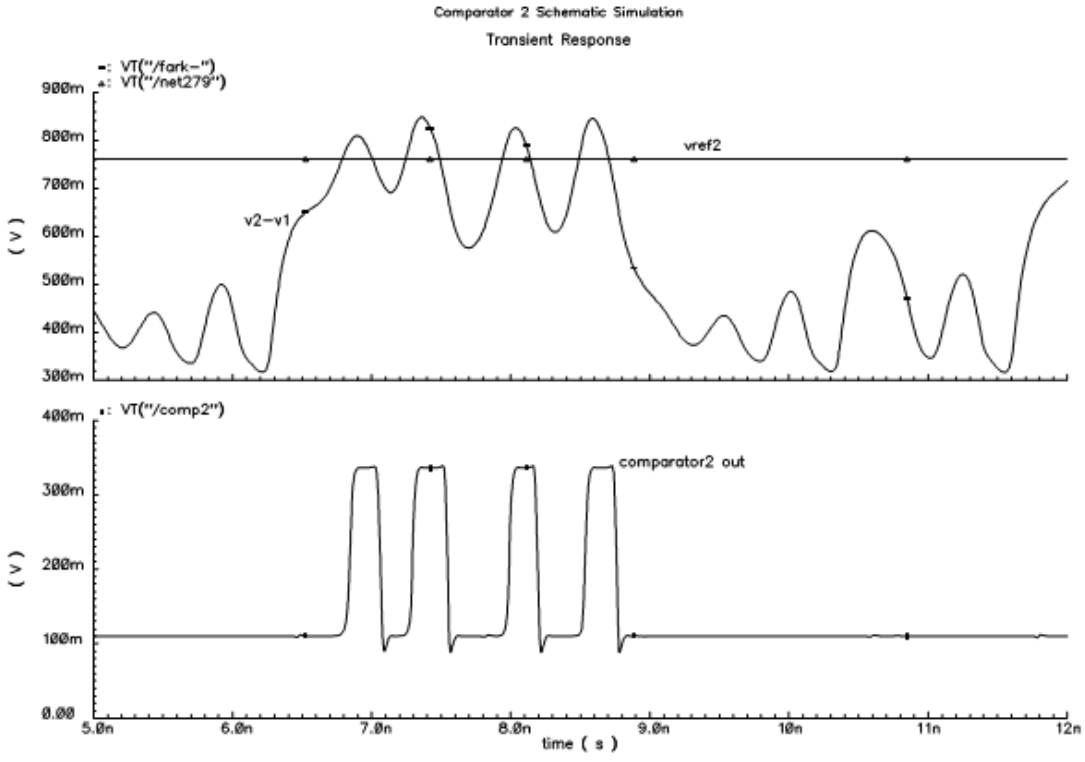

Figure 5.12: Second comparator circuit simulation results

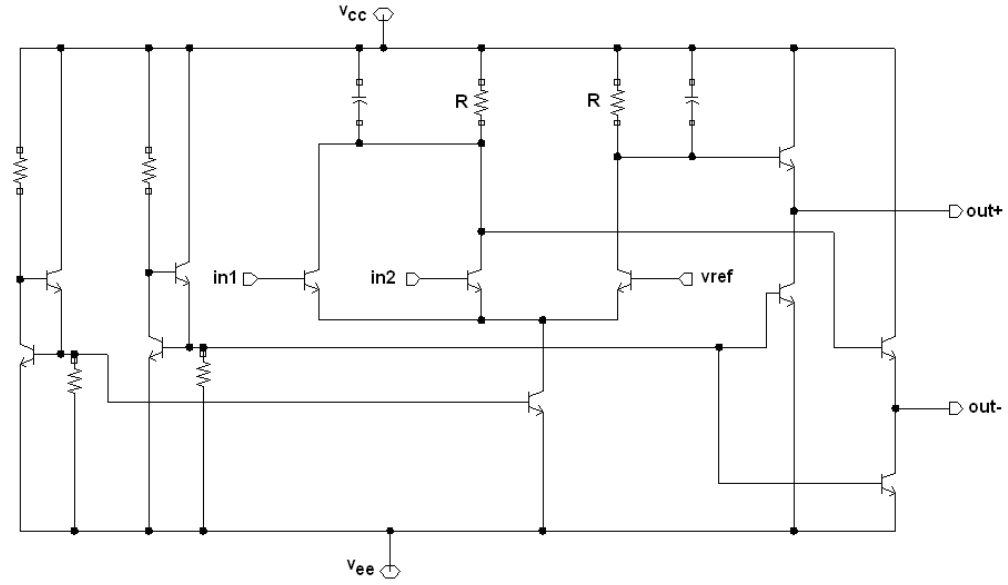

Figure 5.13: Or gate schematic

OR gate's simulation results are shown in Figure 5.14. First two waveforms are inputs and last waveform is output of the OR gate. From Figure it is seen that OR gate is operating correctly. Only when two inputs are zero output is also zero and otherwise output is always one. Output propagation delay is 90 ps.

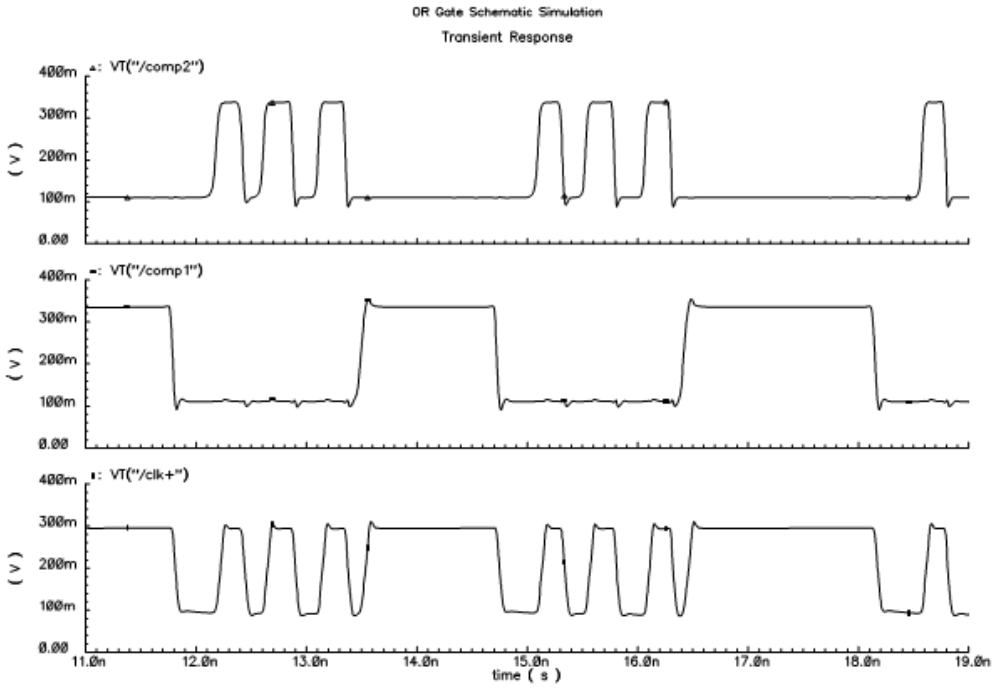

Figure 5.14: Or gate schematic simulation results

5.6 D Type Flip-flop

D-type flip-flop circuit shown in Figure 5.15 is a current mode logic type (CML type) DFF circuit. Resistance values are 400Ω and tail currents are 600μA, respectively.

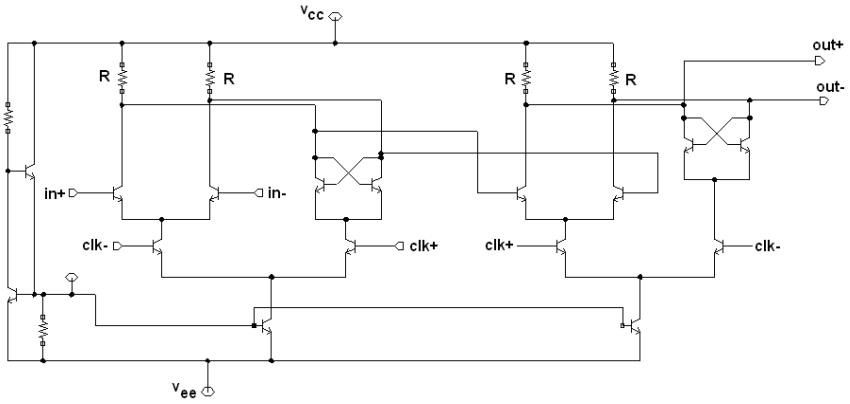

Figure 5.15: DFF circuit schematic

DFF circuit simulation results are shown in Figures 5.16-17. At clock signal's rising edges, input data seen in middle waveform is transferred to the output of the DFF circuit. First waveform is clock input and third waveform is output of the DFF circuit. Glitch levels at the output of the DFF circuit occurring from clock transitions are not as high as that can degrade the functionality of the circuit.

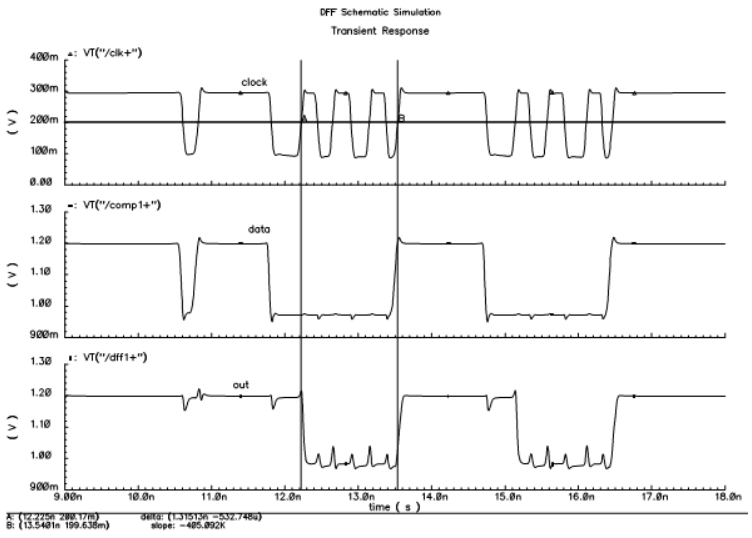

Figure 5.16: DFF schematic simulation results

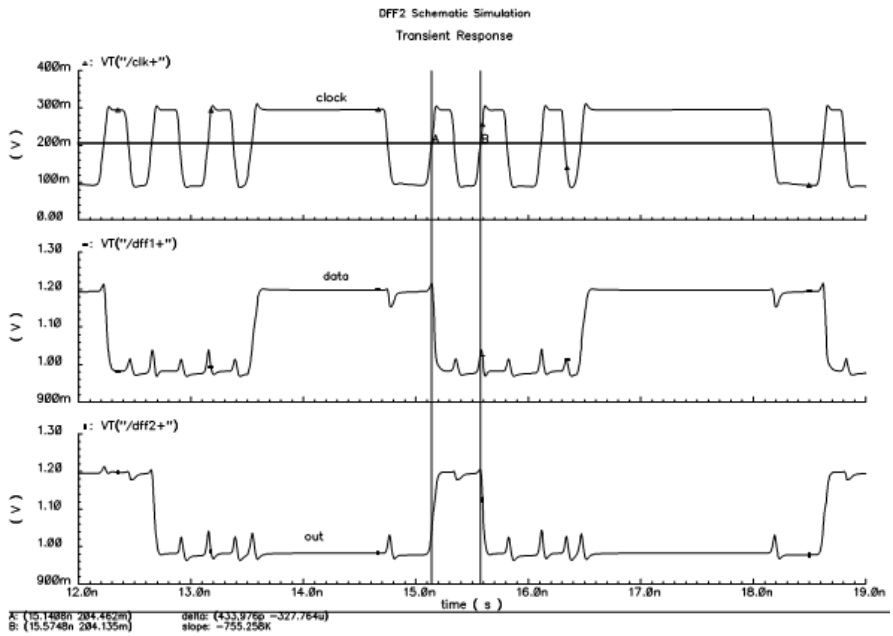

Figure 5.17: Second DFF schematic simulation results

5.7 Divide-by-two circuit

Block diagram of the divide by two circuit is shown in Figure 5.18.

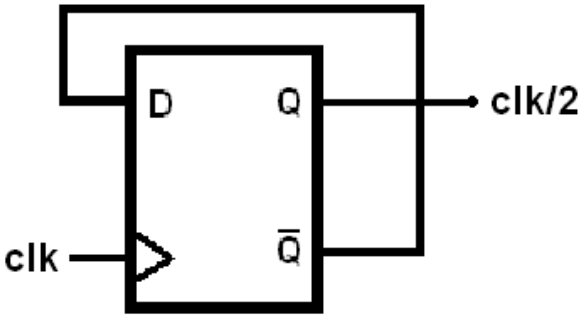

Figure 5.18: Divide by two circuit block diagram

Designed D type flip-flop circuit is used with a synchronous feedback loop as shown in Figure 5.18. Simulation results are given in Figure 5.19.

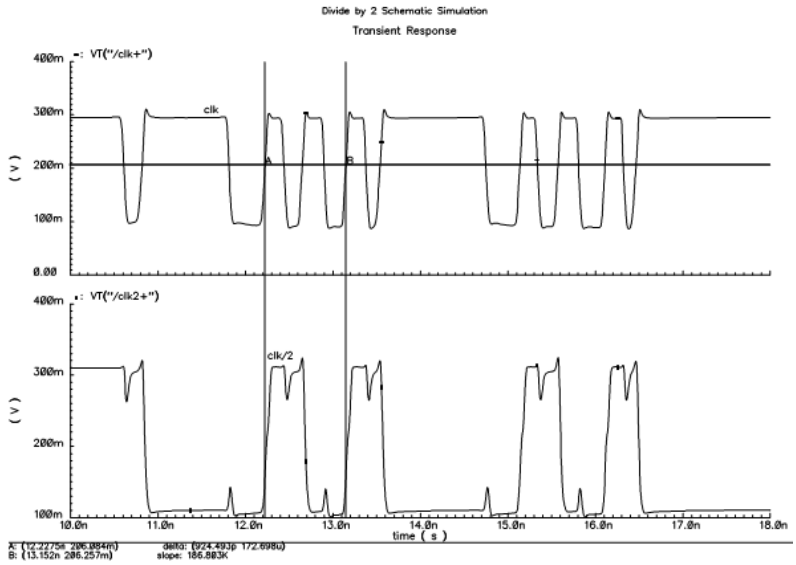

Figure 5.19: Divide-by-two circuit schematic simulation results

First waveform is input and second waveform is output of the divide by two circuit. It is seen that from Figure 5.19 that, the output signal period of the divide by two circuit is two times of its input signal period, therefore the output signal frequency is half of the input signal frequency.

5.8 Exor gate

CML type exor gate schematic is shown in Figure 5.20. Resistance values are 400Ω and tail current of the gate is 600µA, respectively.

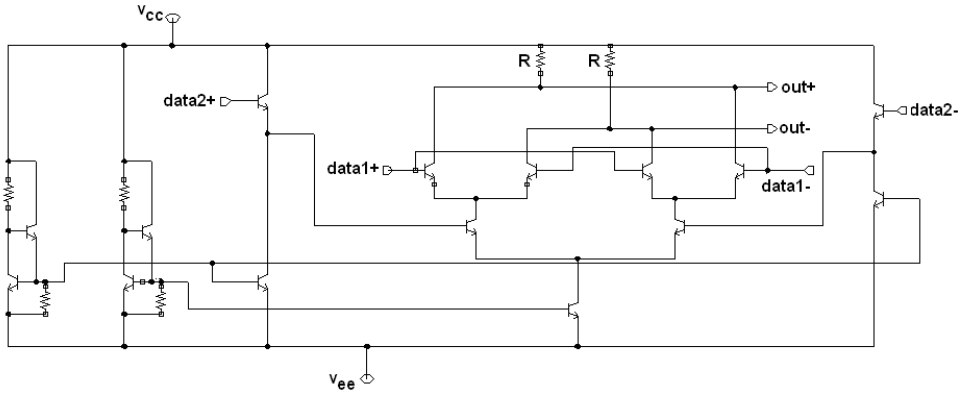

Figure 5.20: Exor gate schematic

Exor gate schematic simulation results are shown in Figure 5.21. First two waveforms are the inputs and third waveform is the output of the Exor gate. When

both two inputs are zero or one, output is zero and when both inputs are complement of each other, exor gate's output is one as seen from Figure 5.21.

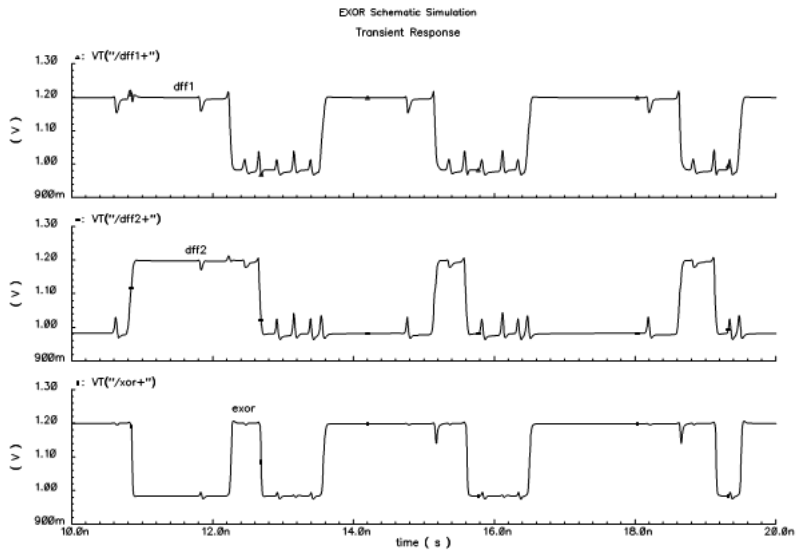

Figure 5.21: Exor circuit simulation results

5.9 CML Pad Drivers

Random number generator block's interface to outside was provided via CML pad drivers with on-chip 50Ω termination resistors. Output drive current is 8mA and swing level is 400mV_{pp}, respectively.

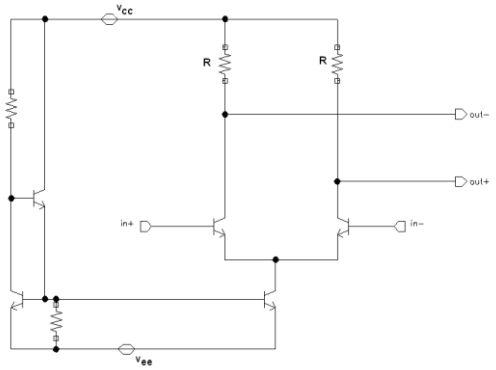

Figure 5.22: CML output pad driver schematic

Simulation setup of CML pad drivers is shown in Figure 5.23 which includes pad and package parasitics such as bondwire inductance and resistance, pin-pad capacitances. Bondwire inductance value is 5nH, its series resistance is 5Ω, pad

capacitance is 100fF and pin capacitance is 5pF. Simulation results are shown in Figure 5.24.

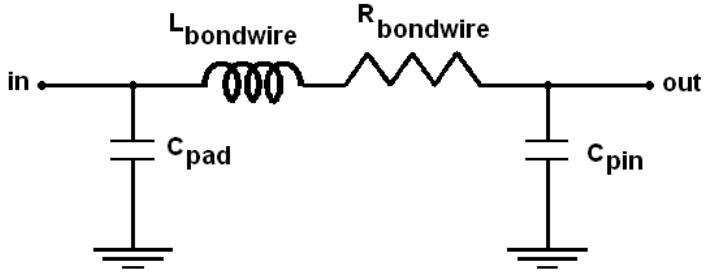

Figure 5.23: Pad and package parasitics

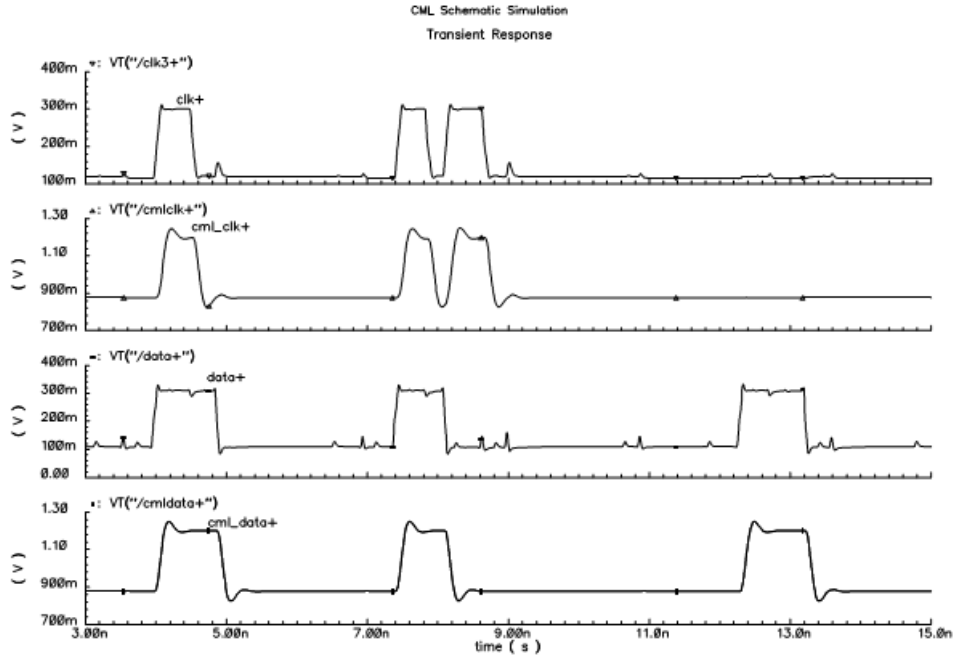

Figure 5.24: CML output pad drivers schematic simulation results

First waveform is the input and second waveform is the output of the circuit in Figure 5.23 which is being driven by a CML gate. It is seen from Figure 5.24 that CML gate can drive its output load successfully with no excess ringing.

5.10 Top level simulations

Chaotic oscillator circuit and random number generation block are simulated and verified to operate correctly in Worst, Typical and Best Case Speed corners. Temperature was swept from -20^{0}C to 50^{0}C during simulations. The entire system

consumes 201.6mW power (20mA at the core circuits and 64mA at CML IO pad drivers from 2.4V power supply). Top level simulation results from schematic are shown in Figure 5.25 at 50^0C temperature. Average throughput of the system is 300Mbits/s. In Figure 5.25, random bit generator outputs from CML gates that are driving pin capacitances are shown.

150.000 bits were taken from Spectre simulations from random number generation system. Each 20.000 bits were subjected to FIPS-140-1 tests and they only fail the poker test. Although chaotic behavior is complex, it needs real device and thermal noise mixing mechanism to generate real random bits. It is thought that, after fabrication of the test chip, generated bit streams will pass all tests.

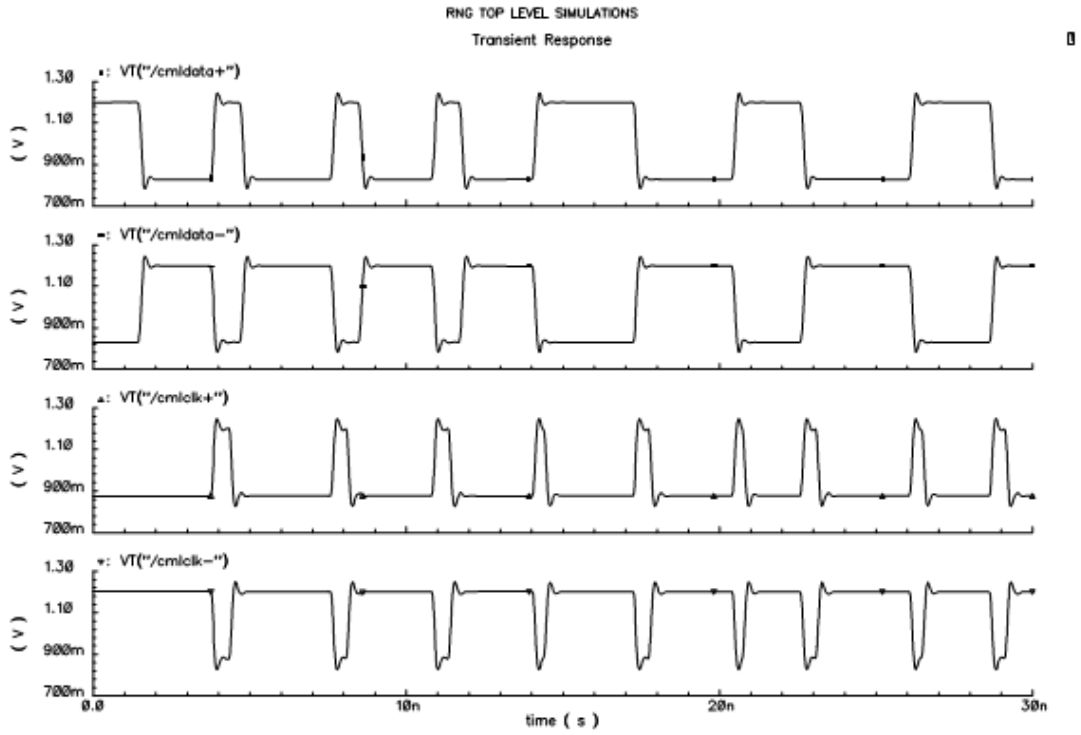

Figure 5.25: Top level simulations

5.11 Circuit layout

System layout was done with IHP's SGB25VD process design rules. Integrated analog tunable resistor structure explained in Section 5.2 was not included in top level layout of the system in order to not to take risk. From spectre simulations, it is observed that when component values deviate because of process variations, changing I_B current is enough to enter chaotic operation regime. All currents of

chaotic oscillator are supplied to chip from pins externally in order to control chaotic operation. Layout is shown in Figure 5.26. Chip layout area is 1mm x 0.5mm.

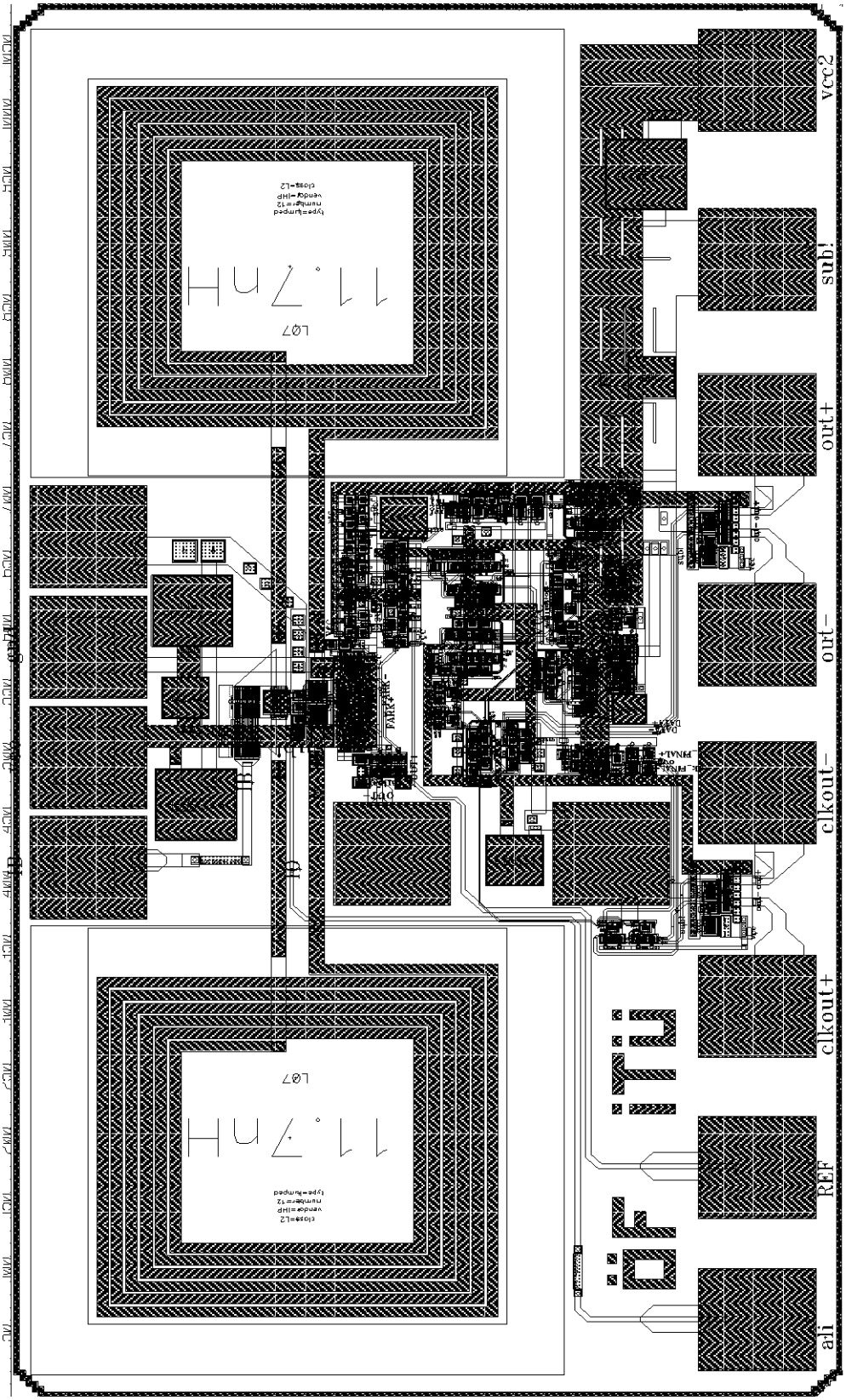

Figure 5.26: Toplevel layout of the system

RF probe pads were placed at difference amplifier outputs to observe time domain chaotic oscillations. Coupling capacitances were placed between V_{CC} and V_{EE} supply lines to decrease power and ground bounce noise. Also different power supply pins were used for chaotic oscillator and other circuitry to prevent coupling between digital circuits and chaotic oscillator through supply lines. Design has been sent to fabrication in IHP's SGB25VD 0.25µm BiCMOS process via Europractice MiniAsic Programme. Test chip bonding diagram is shown in Figure 5.27.

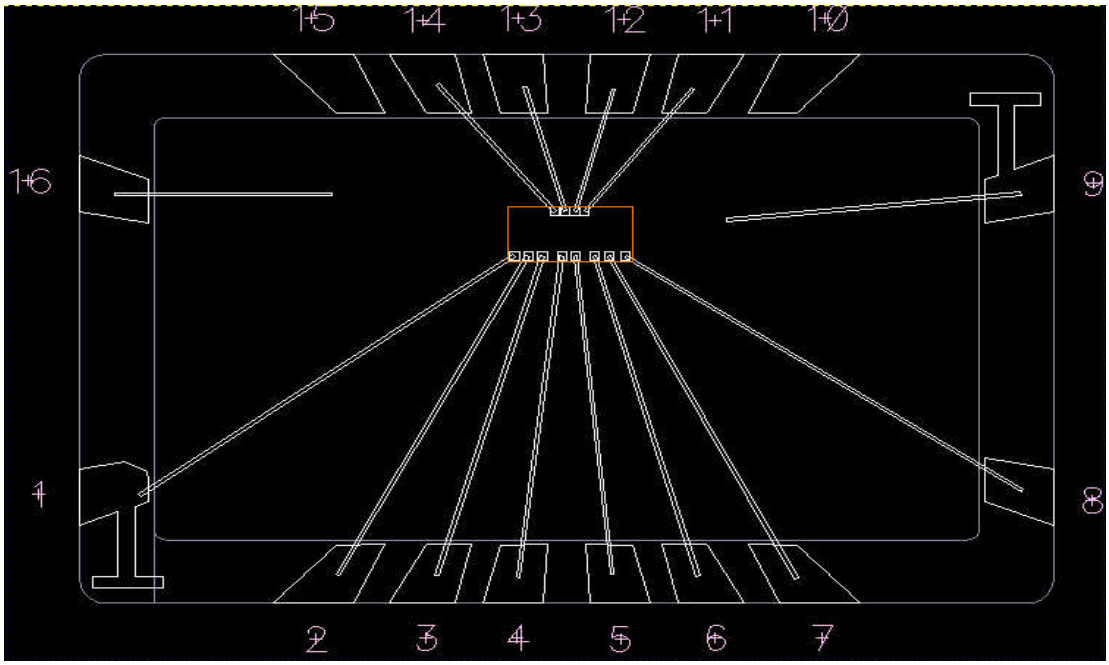

Figure 5.27: Test chip bonding diagram

6. CONCLUSION

The goal of this thesis is to design a high speed chaotic oscillator and utilize it as a high speed random number generator. Achieved throughput of random bit generation system is approximately 300Mbit/s and there are a few reported RNG in the literature around this throughput rate. Also there is no reported chaotic oscillator in the literature operating at same frequencies as our design.

Chaotic oscillator circuit and random number generation block are simulated and verified to operate correctly in Worst, Typical and Best Case Speed corners. Temperature is swept across -20^0C to 50^0C during simulations. Entire system consumes 201.6mW power, 20mA at the core circuits and 64mA at CML IO pad drivers from 2.4V power supply.

System layout was done with IHP's SGB25VD process design rules. Chip layout area is 1mm x 0.5mm. An integrated analog tunable resistor structure that can operate at high frequencies was designed, however it was not included in top level layout of the system in order to not to take risk. From spectre simulations, it is observed that when component values deviate because of process variations, changing I_B current is enough to enter chaotic operation regime. All currents of chaotic oscillator are supplied to chip from pins externally in order to control chaotic operation. RF probe pads were placed at difference amplifier outputs to observe time domain chaotic oscillations in the layout of the system.

Chaotic circuit and random bit generation block was experimentally tested with discrete components at laboratory. Bit streams were acquired using the parallel port of a personal computer. A bit stream of length 1,500,000 was acquired. This bit stream is grouped in 75 groups of bit sequences, each having a length 20,000 bits and each block is subjected to FIPS-1-140 test suit. The first 27 blocks passed the statistical tests. However, 5 of the following 48 blocks fail in the tests. It is thought that this is due to the temporary improper operation of the chaotic oscillator because of external influences due to improper setup. Although, integrated circuit implementation of this circuit may reduce external influences. Finally, we have obtained another bit stream by first grouping the above bit stream in pairs, then

taking first bit of every bit pair. This fact seems to improve the statistical property of the RNG as all the blocks passed the statistical tests of the test suit.

Future work includes testing of chaotic oscillator based random number generator chip, verifying circuit is operational at high frequencies as expected from simulations and generated bit streams pass randomness tests. In this primer work, a smaller inductance value is not chosen in order to not operate at very high frequencies. It is possible to use different chaotic oscillator's differential equation's parameter values a, c_B, c_S, c_O that generate chaos and also different circuit element's values such as inductances and capacitances' values. Chaotic oscillator was verified to be operational at 5GHz frequencies with Spectre simulations. After successfully testing designed chip, a new chaotic oscillator with smaller inductance value and higher operating frequency could be designed and fabricated with different chaotic oscillator's parameter values. Also, an appropriate circuit should be designed to control current sources in the chaotic oscillator to keep oscillator operate in chaotic regime against process and temperature shifts.

REFERENCES

[1] **Yalcin, M.E. , Suykens, J.A.K. and Vandewalle J.,** 2004. True Random Bit Generaton from a Double Scroll Attractor, *IEEE Transactions on Circuits and Systems I : Fundemantal Theory and Applications*, 51, 1395-1404.

[2] **Chua, L.O., Wu, C.W.**, **Huang A. and Zong G.,** 1993. A Universal Circuit for Studying and Generating Chaos – Part I : Routes to Chaos, *IEEE Transactions on Circuits and Systems I : Fundemantal Theory and Applications*, 40, 732-744.

[3] **Menezes, A.J., Van Oorschot, P.C.**, **and Vanstone S.A.,** 1997. Handbook of Applied Cryptography. CRC Press, Florida.

[4] **Craig, S.P. and Connelly J.A.,** 2000. A Noise-Based IC Random Number Generator for Applications in Cryptography, *IEEE Transactions on Circuits and Systems I : Fundemantal Theory and Applications*, 47, 615-621.

[5] **Holman, W.T., Connelly, J.A. and Dowlatabadi A.B.,** 1997. An Integrated Analog/Digital Random Noise Source, *IEEE Transactions on Circuits and Systems I : Fundemantal Theory and Applications*, 44, 521-528.

[6] **Cryptography Research Inc.,** 2003, Evaluation of VIA C3 Nehemiah Random Number Generator, Cryptography Research Inc.

[7] **Yasuda, S., Satake H., Tanamoto T., Ohba R., Uchida K. and Jujita S.,** 2004. Physical Random Number Generator Based on MOS Structure After Soft Breakdown, *IEEE Journal of Solid State Circuits*, 39, 1375-1377.

[8] **Kennedy, M.P.,** 1993. Three Steps to Chaos - Part I: Evolution, *IEEE Transactions on Circuits and Systems I : Fundemantal Theory and Applications*, 40, 640-656.

[9] **Delgado-Restituto, M., Rodriguez-Vazquez, A.,** 2002. Integrated Chaos Generators, *Proceedings of the IEEE*, 90, 747-767.

[10] **Elwakil, A.S. and Kennedy M.P.,** 2001. Construction of Classes of Circuit-Independent Chaotic Oscillators Using Passive-Only Nonlinear Devices, *IEEE Transactions on Circuits and Systems I : Fundemantal Theory and Applications*, 48, 289-307.

[11] **Ozoguz, S., Ates, O., Elwakil, A.S.,** 2005. An Integrated Circuit Chaotic Oscillator and Its Application for High Speed Random Bit Generation, *IEEE Proceedings of the 2005 International Symposium on Circuits and Systems* , Kobe, Japan, May 23-26.

[12] **Razavi, B.,** 2000**.** Design of Analog CMOS Integrated Circuits, McGraw-Hill Companies Inc., New York.

[13] **Conrad, H.,** 1997. 2.4 Gbit/s CML I/Os with integrated line termination resistors realized in 0.5 μm BiCMOS technology, *IEEE Proceedings of the Bipolar/BiCMOS Circuits and Technology Meeting*, Minneapolis, USA, September 28-30.

[14] **Sekerkiran, B.,** 2005. Personal talk.

BIOGRAPHY

Erdoğan Özgür Ateş was born in Istanbul, TURKEY in 1979. He graduated from Haydarpasa Anatolian High School in 1997. In 2002, he received B.Sc. degree in Electronics and Communication Engineering from Istanbul Technical University where he started to continue M.Sc. degree in the same year. He has been working as a research and teaching assistant at the Electronics and Communication Engineering Department of Istanbul Technical University and as a design engineer of industrial ASICs at ETA ASIC Design Center, Istanbul. His research interests are analog and digital high frequency circuit design and digital VLSI design.