Developments of CMOS based Chaotic Oscillator Circuits and Its Application

by

Nattagit Jiteurtragool

Student ID Number: 1198003

A dissertation submitted to the
Engineering Course, Department of Engineering,
Graduate School of Engineering,
Kochi University of Technology,
Kochi, Japan

in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

Assessment Committee:
Supervisor: TACHIBANA Masayoshi
Co-Supervisor: MITSUYAMA Yukio
IWASHITA Katsushi
IWATA Makoto
HAMAMURA Masanori

September 2018

Abstract

Over the past decade, chaos theory has been purely studied for academic as a fascinating mathematical phenomenon, until latterly a new research aspect has emerged. As a result of many years of research and study, chaos has now been considered beneficial to actual applications especially in communication and cryptography. Regarding to the increasing interest on chaos, a circuit which offer chaotic behavior such a chaotic oscillator circuit has become a subject of increasingly and extensively research and study and led to an introduction of many new design chaotic oscillator circuits.

Beside the increasing interest in research on chaotic oscillator, a major part of cryptography such a true random number generator has also recently attracted a lot of research attention due to the increasingly demand on security and privacy. Typically, the true random number generator is utilized in confidential key generation, however it can also be used in some computational algorithm. Although the dynamics of chaotic systems is deterministic, the highly sensitivity to change of initial condition and aperiodic characteristic of the chaotic system still make chaotic oscillator suitable for the use as a randomness source of true random number generator.

This dissertation mainly aims to develop new chaotic oscillators as well as research and investigation on new chaotic maps and their chaotic dynamic. The circuit structures of the oscillators are expected to be simple and compact, yet proper chaotic dynamics such a robustness are also expected. The design strategy for the chaotic oscillator is the development of circuit regarding the exiting chaotic maps and the new

propose chaotic maps. Hence, the implementation of application regarding chaotic oscillators such a true random number generator is also develop as a practical example. Through the literature reviews, a hypothesis can be defined that the chaotic oscillator circuit can be built by using a nonlinear circuit with the specific transfer characteristic. The first topic of study is to design new chaotic oscillators using nonlinear circuit with V-shape and S-shape (sigmoid) characteristic in order to prove the hypothesis. The second and third topics are aim to study and develop two new chaotic maps based on sigmoidal function and parabolic function. The results of the study from both chaotic maps show the feasibility of offering robust chaotic.

As mentioned, the first study presents two CMOS based discrete-time chaotic oscillators and its application for random number generator (RNG). The first design method of chaotic oscillator was given by the use of 3 transistors to construct chaotic map circuit in order to achieve a V-shape characteristic (inverse tent map). Simulation of the chaotic oscillator is described and examined in terms of bifurcation diagram and transient waveform to show that it has a desirable output and suitability for a true random number generator (TRNG). The TRNG is designed using chaotic oscillator as random signal generator which also known as entropy source and randomness of output signal can be increased by a dual oscillator sampling method and a XOR operation. The second design method of chaotic oscillator is based on a chaotic map with reverse sigmoid characteristic. Then, a hybrid random number generator (HRNG) based on a combination of discrete-time chaotic oscillator and a linear feedback shift register (LFSR) is presented. A random signal is produced by the chaotic oscillator and then, to increases the randomness; the signal is combined with LFSR signal through XOR gate. The resulting output from both RNG are evaluated using the NIST SP800-22 test suite.

The second study is interested regarding a sigmoidal chaotic map, which has never been distinctly investigated. A generic form of the sigmoidal chaotic map with three terms, i.e., $x_{n+1} = \mp A f_{NL}(Bx_n) \pm Cx_n \pm D$, where A, B, C, and D are real constants is introduced. The unification of modified sigmoid and hyperbolic tangent (tanh) functions reveals the existence of a "unified sigmoidal chaotic map" generically fulfilling the three terms, with robust chaos partially appearing in some parameter ranges. A simplified generic form, i.e., $x_{n+1} = \mp f_{NL}(Bx_n) \pm Cx_n$, through various S-shaped functions, has recently led to the possibility of linearization using (i) hardtanh and (ii) signum functions. This study finds a linearized sigmoidal chaotic map that potentially offers robust chaos over an entire range of parameters. Chaos dynamics are described in terms of chaotic waveforms, histogram, cobweb plots, fixed point, Jacobian, and a bifurcation structure diagram based on Lyapunov exponents. Hence, the chaotic oscillator based the linearized sigmoidal chaotic map is shown as well as a true random number generator based on the proposed chaotic oscillator is demonstrated as a practical example. The resulting output of the random number generator is evaluated using the NIST SP800-22 test suite and TestU01.

As the proposed generic form of chaotic map is introduced in the study of sigmoidal chaotic map, the third study is interested in introducing a new chaotic map based on nonlinear function with parabola curve transfer characteristic. A parabola chaotic map is based on various parabola curve functions which led to the linearized parabola chaotic map using. The linearized chaotic map can of offer a robust chaos over the entire range of parameter. Chaos dynamics were described in terms of fixed point, Jacobian, chaotic waveforms, cobweb plots, bifurcation diagram, and Lyapunov exponents. A discrete-time chaotic oscillator circuit based on the proposed parabola

chaotic map is presented. Simulation results of the circuit such a bifurcation diagram and chaotic waveforms are presented in order to investigate the chaotic dynamic of the circuit which also revealed that the proposed chaotic oscillator can offer robust chaos nearly the entire range of parameter.

The proposed circuits show that chaotic oscillator can be achieved by using a simple structure with specific transfer characteristic such as V-shape or S-shape (sigmoid) characteristic and the simulation results show the feasibility and compatibility as a randomness source for true random number generator. The conclusion of the proposed chaotic oscillators is led to the proposed chaotic maps which based on sigmoidal function and parabolic function. Furthermore, the proposed chaotic maps based on the linearized functions have demonstrated the robustness property of chaotic system.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

For a long time, chaos theory has only been research and study mainly for the academic purpose. Up until lately where there has been remarkable interest of using chaos in many actual applications. As a result, circuit design and implementation of nonlinear systems which offer chaotic behavior such a chaotic oscillator have been increasingly and widely study. Cryptography application can be considered one of the applications that chaotic oscillator is suited for. The random number generator which is the key to most of cryptography application is now received increasingly interested in as well as the chaotic oscillator.

This chapter initially introduces chaos theory, chaotic dynamic measurement tools and random number generator. The motivation and objective of this dissertation are included. Thesis organization is finally summarized.

1.1 Chaos Theory

Chaos theory is the study in complicated mathematical regarding to the behavior of nonlinear dynamical systems. While most traditional scientific theory is the study of predictable phenomena like gravity, electricity, or chemical reactions, nonlinear dynamical systems are highly sensitive to initial conditions and unpredictable. The chaos

theory explores the effects of small occurrences dramatically affecting the outcomes of seemingly unrelated events.

In the early 1960s, Chaos theory was discovered and experimental by Edward Lorenz, a mathematician and meteorologist, who was working with a system of equations to theoretically model and predict weather conditions. He began to realize that seemingly insignificant factors in a dynamic system such as the atmosphere or a model of the atmosphere could cause vast and often unsuspected results.

Chaotic behavior exists in many natural systems, such as weather and climate. This behavior can be studied through analysis of a chaotic mathematical model, or through analytical techniques such as recurrence plots and Poincaré maps. Although no universally accepted mathematical definition of chaos exists, commonly used properties for a dynamical system to be classified as chaotic are:

- All chaotic systems have an extremely sensitive to the initial conditions.
- The trajectory of systems never repeats.
- All chaotic systems are nonlinear.

Hence, Chaos is aperiodic long-term behavior in a deterministic system that exhibits sensitive dependence on initial conditions [1]. Classical example of the chaotic behavior is Brownian motion, change of the weather, behavior of the financial markets, the biological processes in the living organisms, the fluctuation of the astronomical orbit, etc.

For a long time, the study of chaotic circuits has generally been purely for academic and theoretical reasons. Chaotic circuits were built as physical tools to study the nonlinear dynamics described by a set of governing equations. Mathematicians and theoretical physicists built chaotic circuits to explain the dynamics of complex systems,

though engineers usually see chaotic behavior as an undesirable effect to be avoided in designed systems until recently. Through an extensively research and study for decade, a new perspective of chaos shows that chaos may offer substantial benefits many applications [2-10], including communications, remote sensing, and cryptography. As a result, many new types of chaotic oscillators are increasingly being introduced to meet the needs in such applications [11-17].

1.2 Chaotic Measurement

In order study chaotic system, there are many tools that can be employed. However, to preliminary investigate the chaotic behavior there are 2 measurement tools that widely used such as the bifurcation diagram and the Lyapunov Exponents (LE) [18-20]. The bifurcation diagram is admittedly accepted as a tool for qualitative measure which shows the possible long-term values of a system. Depending on the initial conditions of the system, the behavior can follow different branches to chaos. The example of chaotic maps which is the most well-known and widely used in many areas of applications is a logistic map [21] and the logistic equation is written as follows

$$x_{n+1} = r x_n \left(1 - x_n\right) \tag{1.2}$$

Fig.1.1 depicts the plot of bifurcation diagram of the Logistic map showing effects of the parameter r in the equation, a periodic system will have one point while a system exhibiting period doubling will have two points and a chaotic system will have multiple points. The thick region can be considered a chaotic region and the existing of periodic windows between chaotic region indicate whether its robust chaos or not.

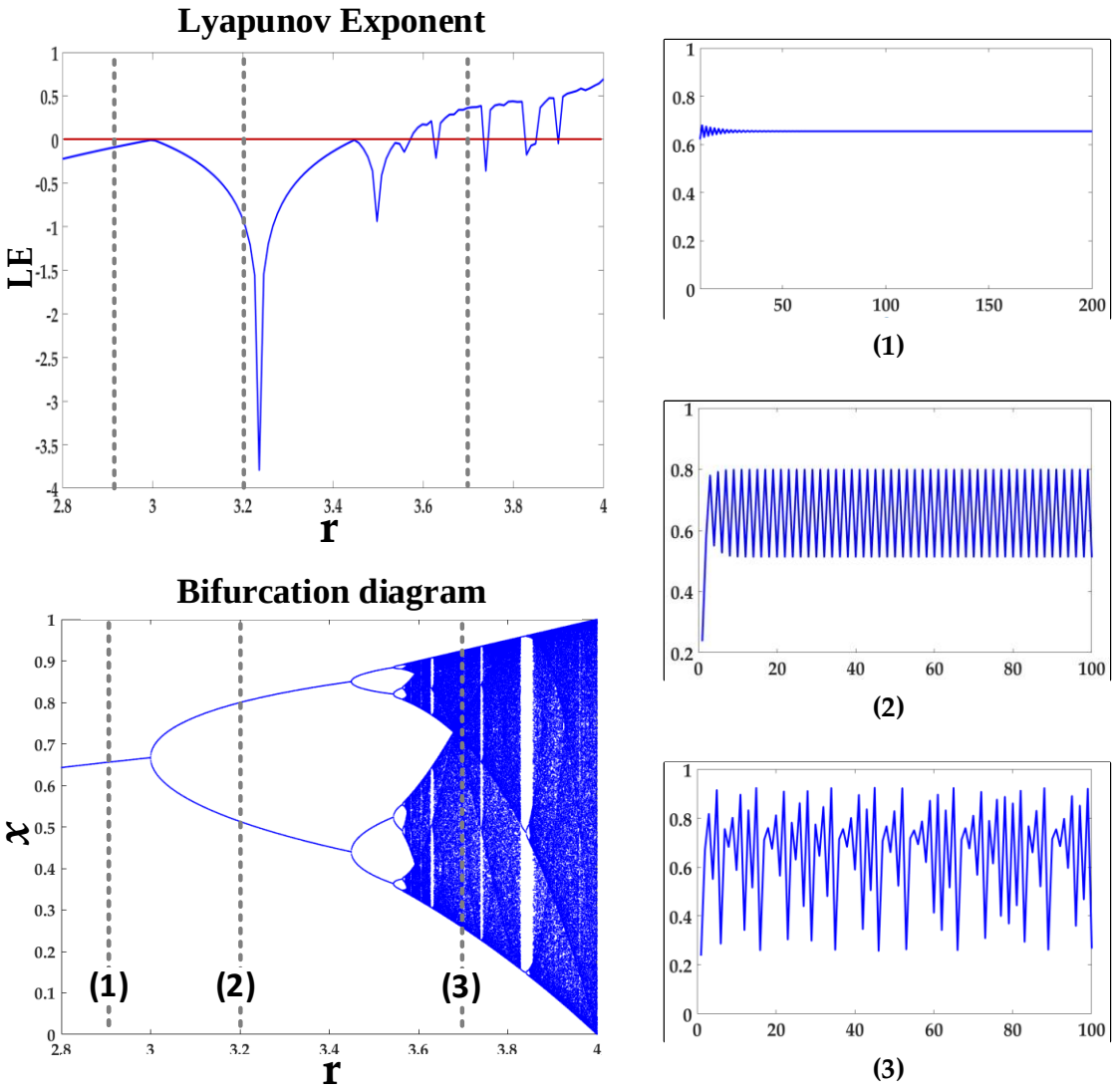

Figure 1.1 The plot of Lyapunov Exponents (LE) and bifurcation diagram of the Logistic map showing effects of the parameter r.

On the other hand, the LE is admittedly and widely used as a tool for quantitative measurement. The LE is defined as a quantity that characterizes the rate of separation of infinitesimally close trajectories and is given by

$$\mathrm{LE} = \lim_{n\to\infty} \frac{1}{N} \sum_{n=1}^{N} \log_2 \frac{dX_{n+1}}{dX_n} \tag{1.1}$$

where N is the number of iterations Typically, the positive LE, indicates chaotic behaviors of dynamical systems and the larger value of LE results in higher degree of chaoticity.

Other than the investigation on chaotic dynamic using quantitative and qualitative tools such a LE and bifurcation diagram, chaotic dynamic can be investigated using the Jacobian [22], which can be calculated through a first derivative as $|J(x_n)| = f'(x_n)$. Typically, the discrete time system becomes unstable in the condition of $|J(x_n)| > 1$, while the chaotic map needs to operate under an unstable condition in order to induce the chaos.

1.3 Random Number Generator

A Random Number Generator (RNG) is a computational or physical device designed to generate a sequence of numbers which randomness. Random numbers are useful for a variety of purposes in many fields of application, such as generating data encryption keys, statistical sampling, simulating and modeling complex phenomena and other areas where producing an unpredictable result is desirable.

There are many computational methods for random number generation; nevertheless, it can be classifying into two principal approaches to generate random numbers: Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs). The approaches have different characteristics and its advantages.

1.3.1 Pseudo Random Number Generator

A pseudorandom number generator (PRNG), also known as a deterministic random bit generator, is an algorithm that uses mathematical formulae for generating a sequence of numbers whose properties approximate the properties of sequences of

random numbers. The PRNG-generated sequence is not truly random, because it is completely determined by a relatively small set of initial values, called the PRNG's seed (which may include truly random values).

PRNGs are important for their speed in number generation and their reproducibility which make them suitable for applications where many numbers are required and where it is useful that the same sequence can be replayed easily. The PRNGs are mainly uses in application such as cryptography, simulation and modeling applications, or games.

Characteristic of PRNGs are efficient and deterministic, meaning they can produce many numbers in a short time and a given sequence of numbers can be reproduced if the starting point in the sequence is known. PRNGs are typically also periodic, which means that the sequence will eventually repeat itself.

1.3.2 True Random Number Generator

TRNG is a device that generates random numbers from a physical process, rather than a computer program. TRNGs are often based on measurement from natural phenomena such as atmospheric noise, thermal noise, other external electromagnetic, the photoelectric effect and other quantum phenomena.

The major use for electronic hardware TRNG is in cryptography. TRNGs can produce sequences of numbers that are unpredictable, which is greatest security when used to encrypt data. However, this hardware based random number generators generally produce a limited number of random bits per second which depend on source harvesting.

The characteristics of TRNGs are different from PRNGs. First, TRNGs are generally rather inefficient compared to PRNGs, taking considerably longer time to

produce numbers. They are also nondeterministic which meaning that a given sequence of numbers cannot be reproduced. Lastly, TRNGs have no period, meaning a generated sequence number will not repeat. Table 1.1 shows characteristics of the two types of random number generators. However, many existed TRNGs are implemented using a circuit based chaotic oscillator as a randomness source [23-27]. Though chaotic oscillator theoretically is a deterministic system, the chaotic signal generated from the circuit based chaotic oscillator is a result on many immeasurable parameters such as thermal noise.

Table 1.1 Characteristics of the two types of random number generators

Characteristic	**PRNGs**	**TRNGs**
Efficiency	Fast	Slow
Determinism	Deterministic	Nondeterministic
Periodicity	Periodic	Non periodic

Typically, RNG is consists of 3 part including an entropy source (or randomness source), an entropy harvester, and a post processor as depicted in Figure 1.2. Beside from randomness source, the TRNG also required a post processor as for the purpose of statistical improvement.

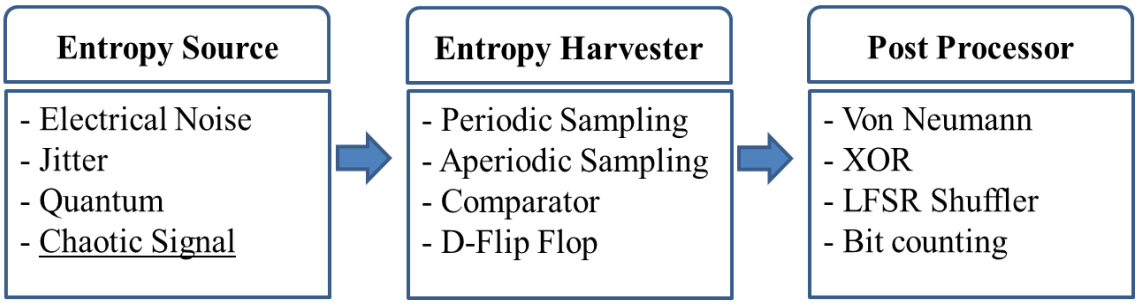

Figure 1.2 Structure of random number generator.

1.4 Statistical Test

Various statistical tests can be applied to a sequence to attempt to compare and evaluate the sequence to a truly random sequence. The properties of a random sequence can be characterized and described in terms of probability. There are an infinite number of possible statistical tests, each assessing the presence or absence of a "pattern" which, if detected, would indicate that the sequence is nonrandom.

The NIST Test Suite from National Institute of Standards and Technology is a statistical package consists of 15 tests which are generally accepted as a standard test suit for any random number generators [28]. NIST were developed to test the randomness of (arbitrarily long) binary sequences produced from random number generators by. Table 1.2 describes the general characteristics of each of the statistical tests.

All the statistical tests attempt to extract the presence of a pattern that indicates non-randomness of the sequences through probability methods described in terms of p-value. For each test in NIST, this p-value indicates the strength of evidence against perfect randomness hypothesis, i.e. a p-value greater than a typical confidence level of 0.01 implies that the sequence is random with a confidence level of 99%.

Another tool for randomness test is TestU01 which is a software library, implemented in the ANSI C language, and offering a collection of utilities for the empirical statistical testing of uniform random number generators [29]. The library was first introduced in 2007 by Pierre L'Ecuyer and Richard Simard of the Université de Montréal. The library implements several types of random number generators, including

some proposed in the literature and some found in widely used software. It provides general implementations of the classical statistical tests for random number generators, as well as several others proposed in the literature. Each statistical test in TestU01 can generate a P-value as well as the NIST test suite, which is considered as an indicator of passing the test.

Table 1.2 Characteristics of the NIST Statistical Tests

Statistical Tests	Descriptions
Frequency (mono-bit)	Too many zeroes or ones.
Frequency Block	Too many zeroes or ones within M-bit blocks.
Runs	Large (small) total number of runs indicates that the oscillation in the bit stream is too fast (too slow).
Longest Run of Ones Block	Deviation of the distribution of long runs of ones.
Binary Matrix Rank	Deviation of the rank distribution from a corresponding random sequence, due to periodicity.
Discrete Fourier Transform (Spectral)	Periodic features in the bit stream.
Non-overlapping Template Matching	Too many occurrences of non-periodic templates
Overlapping Template Matching	Too many occurrences of m-bit runs of ones.
Universal Statistical	Compressibility (regularity).
Linear Complexity	Deviation from the distribution of the linear complexity for finite length (sub) strings.
Serial	Non-uniform distribution of m-length words. Similar to Approximate Entropy.
Approximate Entropy	Non-uniform distribution of m-length words. Small values of ApEn(m) imply strong regularity.

Cumulative Sums	Too many zeroes or ones at the beginning of the sequence.
Random Excursions	Deviation from the distribution of the number of visits of a random walk8 to a certain state.
Random Excursions Variant	Deviation from the distribution of the total number of visits (across many random walks) to a certain state.

1.5 Thesis Developments and Organizations

1.5.1 Objective and Motivation

As the demand on chaotic oscillator is gradually increased during the past decade which led to the research and development of this dissertation. Chaos theory, which exited in many natural phenomena, can also be considered as a very fascinating mathematical and found in many applications through various areas of research. Many existing chaotic oscillator circuits are designed with a complicated circuit structure and required large amount of number of elements. Hence, the design and development of chaotic oscillator with simple and compact structure is needed. Despite many exiting chaotic maps, only a few of those maps have been investigated in term of robustness. The search for new chaotic map with robustness property is also considered. The application with regarding to the chaotic oscillator circuits such a true random bit generator is also interesting.

1.5.2 Thesis Organization

This thesis is organized into five chapters. The following chapter 2 presents the research and study of two CMOS based discrete-time chaotic oscillators and its

application for random bit generator (RBG). The first design approach of chaotic oscillator was given by the use of 3 transistors to construct chaotic map circuit in order to achieve a V-shape characteristic (inverse tent map). Simulation of the chaotic oscillator was described and examined in terms of bifurcation diagram and transient waveform to show that it has a desirable output and suitability for a true random bit generator (TRBG). The TRBG is designed using chaotic oscillator as random signal generator which also known as entropy source and randomness of output signal can be increased by a dual oscillator sampling method and a XOR operation. The second design approach of chaotic oscillator is based on a chaotic map with reverse sigmoid characteristic. Then, a hybrid random number generator (HRNG) based on a combination of discrete-time chaotic oscillator and a linear feedback shift register (LFSR) is presented. A random signal is produced by the chaotic oscillator and then, to increases the randomness; the signal is combined with LFSR signal through XOR gate. The resulting output from both RBG are evaluated using the NIST SP800-22 test suite.

Chapter 3 presents the research and study regarding a 1-D sigmoidal chaotic map, which has never been distinctly investigated. In this chapter, a generic form of the sigmoidal chaotic map with three terms is introduced. The unification of modified sigmoid and hyperbolic tangent (tanh) functions reveals the existence of a “unified sigmoidal chaotic map” generically fulfilling the three terms, with robust chaos partially appearing in some parameter ranges. A simplified generic form through various S-shaped functions, has recently led to the possibility of linearization using (i) hardtanh and (ii) signum functions. This study finds a linearized sigmoidal chaotic map that potentially offers robust chaos over an entire range of parameters. Chaos dynamics are described in terms of chaotic waveforms, histogram, cobweb plots, fixed point, Jacobian, and a

bifurcation structure diagram based on Lyapunov exponents. As a practical example, a true random bit generator using the linearized sigmoidal chaotic map is demonstrated. The resulting output is evaluated using the NIST SP800-22 test suite and TestU01.

Chapter 4 presents the research and study regarding a parabola chaotic map, which has never been distinctly investigated. Regarding the proposed generic form of chaotic map with three terms which introduced in the Chapter 3, a new chaotic map based on nonlinear function with parabola curve transfer characteristic is proposed. A simplified parabola chaotic map is based on various parabola curve functions which led to the linearized parabola chaotic map using Absolute Value function. The linearized chaotic map can of offer a robust chaos over the entire range of parameter. Chaos dynamics were described in terms of fixed point, Jacobian, chaotic waveforms, cobweb plots, bifurcation diagram, and Lyapunov exponents. A discrete-time chaotic oscillator circuit based on the proposed parabola chaotic map is presented. Simulation results of the circuit such a bifurcation diagram and chaotic waveforms are presented in order to investigate the chaotic dynamic of the circuit which also revealed that the proposed chaotic oscillator can offer robust chaos nearly the entire range of parameter.

Chapter 5 finally draws a conclusion of all three approaches of designing chaotic oscillator as well as the research and study of two new chaotic maps. The proposed chaotic oscillators implementation using a simple structure and few numbers of components while maintaining chaotic dynamic and feasibility of utilizing in other applications.

Chapter 2

Chaotic Oscillators based on Transfer Characteristic

This chapter presents the research and study of two CMOS based discrete-time chaotic oscillators and its application for random bit generator (RBG). Through the literature reviews, a hypothesis can be defined that the chaotic oscillator circuit can be construct by using a nonlinear circuit with the specific transfer characteristic such as V-shape or S-shape (sigmoid) characteristic.

The first design approach of chaotic oscillator was given by the use of 3 transistors to construct chaotic map circuit in order to achieve a V-shape characteristic (inverse tent map). Simulation of the chaotic oscillator was described and examined in terms of bifurcation diagram and transient waveform to show that it has a desirable output and suitability for a true random bit generator (TRBG). The TRBG is designed using chaotic oscillator as random signal generator which also known as entropy source and randomness of output signal can be increased by a dual oscillator sampling method and a XOR operation. The second design approach of chaotic oscillator is based on a chaotic map with reverse sigmoid characteristic. Then, a hybrid random number generator (HRNG) based on a combination of discrete-time chaotic oscillator and a linear feedback shift register (LFSR) is presented. A random signal is produced by the chaotic oscillator and then, to increases the randomness; the signal is combined with LFSR signal through

XOR gate. The resulting output from both RBG are evaluated using the NIST SP800-22 test suite.

Firstly, the introduction and overview of discrete-time chaotic oscillators are given. Then, the discrete-time chaotic oscillator circuit based on chaotic map with V-shape characteristic and its application as dual oscillator sampling based true random bit generator are presented. Subsequently, the discrete-time chaotic oscillator circuit based on a chaotic map with reverse sigmoid characteristic and its application as hybrid random bit generator are also presented. Finally, the conclusion is drawn.

2.1 Introduction

Chaotic oscillator is one of the most interesting topics of research and the designing of the circuit been extensively studied for many decades [30-33]. Primary aim of chaotic oscillator design is to construct a circuit that able to provide truly random signals and extremely sensitivity to initial condition or changing parameter as well as a random bit generator.

In general, chaotic oscillator chaotic oscillators can be classified into discrete-time and continuous-time chaotic oscillators. As for continuous-time chaotic oscillators, their differential equations define the future state in terms of the rate of change associated with the current state variables, while the future state of discrete-time chaotic systems is defined by the difference equations depends only on the value of current state. Even though the continuous-time chaotic oscillators have been studied for decade, in circuit design, most of continuous-time chaotic oscillators usually implemented using resistor-capacitor network or an inductor which required a large area of circuit. While discrete-time chaotic systems have been attracted more attention due to their numerous techniques

to design while remain capability of complex and chaotic behavior. Thus, the compact structure discrete-time chaotic oscillator circuits with feasibility to produce a robust chaotic signal for some partial portion of parameter space are presented.

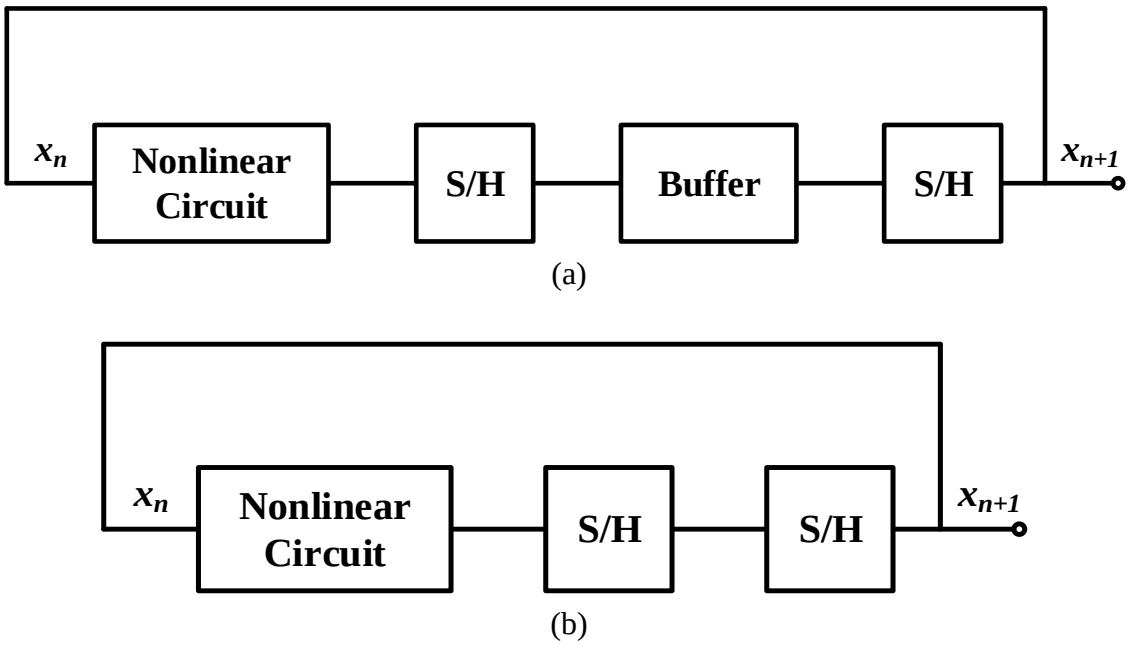

Figure 2.1 Discrete-time chaotic oscillator (a) with buffer, (b) without buffer.

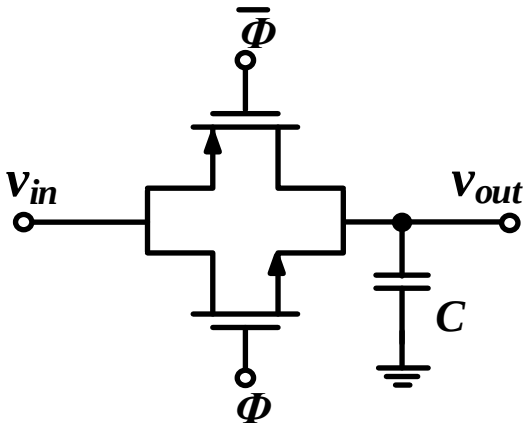

Figure 2.2 The sample and hold circuit using transmission gate.

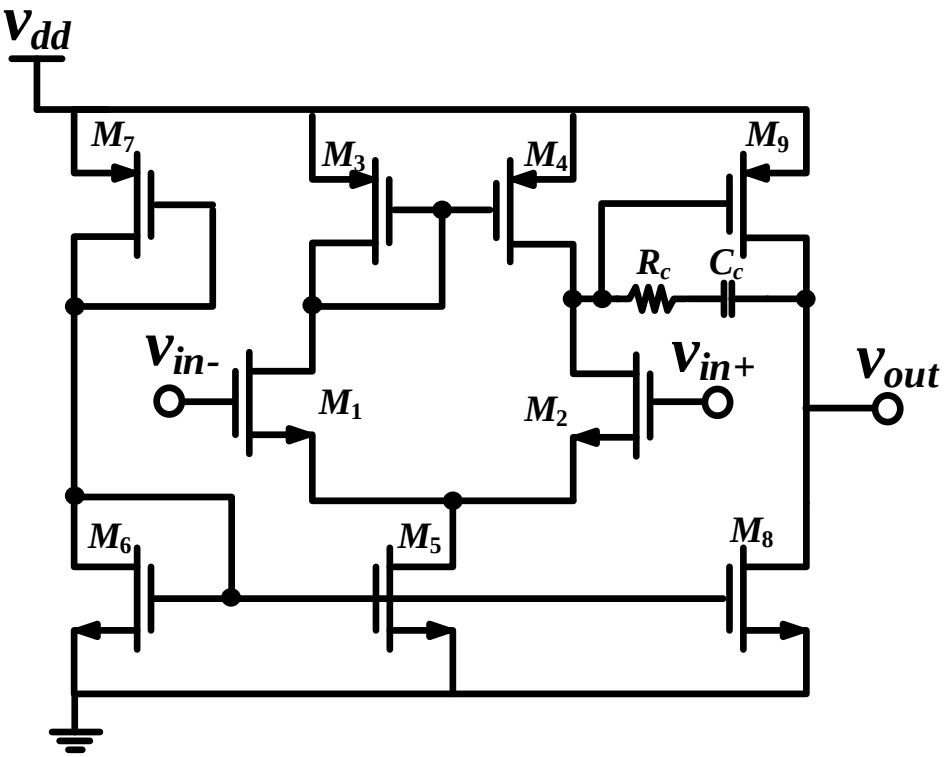

Figure 2.3 Circuit diagram of the proposed two-stage Op Amp circuit.

Discrete-time chaotic oscillator can generate chaotic signals though a nonlinear iteration function (chaotic map) which can be defined as follows:

$$X_{n+1} = f(X_n) \tag{2.1}$$

Typically, a discrete-time chaotic oscillator can be designed using a common structure [34] as shown in Figure 2.1. In addition to a nonlinear (chaotic map) circuit, the chaotic oscillator requires two sample and hold circuits as depicted in Figure 2.1a, and occasionally, also requires a buffer between the sample and hold as shown in Figure 2.1b. The sample-and-hold circuits are used to delay the signals similar to the memory, and the buffer circuit is used to feed signals into the next iteration. Both of the proposed chaotic oscillator is designed based on the structure of chaotic oscillator based on Figure 2.1a. The buffer circuit and the sample and hold circuit of the proposed chaotic oscillator in

this chapter are implemented by sample and hold circuit using transmission gate and two-stage operational amplifier (Op Amp) as shown in Figure 2.2 and Figure 2.3 respectively. The element sizes and performance of the Op Amp are listed in Table 2.1 and Table 2.2 respectively.

Table 2.1 Elements parameter of the proposed two-stage Op Amp circuit.

Elements	**Size (µm)**
M1, M2	2/0.18 W/L(µm)
M3, M4	4/0.18 W/L(µm)
M5	1.2/0.18 W/L(µm)
M6	4/0.18 W/L(µm)
M7	1.2/0.18 W/L(µm)
M8	1.2/0.18 W/L(µm)
M9	10.8/0.18 W/L(µm)
M10	5.4/0.18 W/L(µm)
R_c	2.5 kΩ
C_c	0.5 pF

Table 2.2 Performance simulation of the proposed two-stage Op Amp circuit.

Performance	**Values**	**Units**
Offset voltage	57	µV
DC gain	70	dB
Phase margin	67	Degree
Slew rate	+56/-44	µV/S
ICMR	0.55-1.75	V

2.2 Discrete-Time Chaotic Oscillator: V-shape Transfer Characteristic

Numerous discrete-time chaotic oscillator circuits are proposed using the design technique of imitating V-shape or N-shape nonlinear transfer function of the chaotic oscillator [35-38]. This technique is effective to provide the robust chaotic signals in both voltage and current mode.

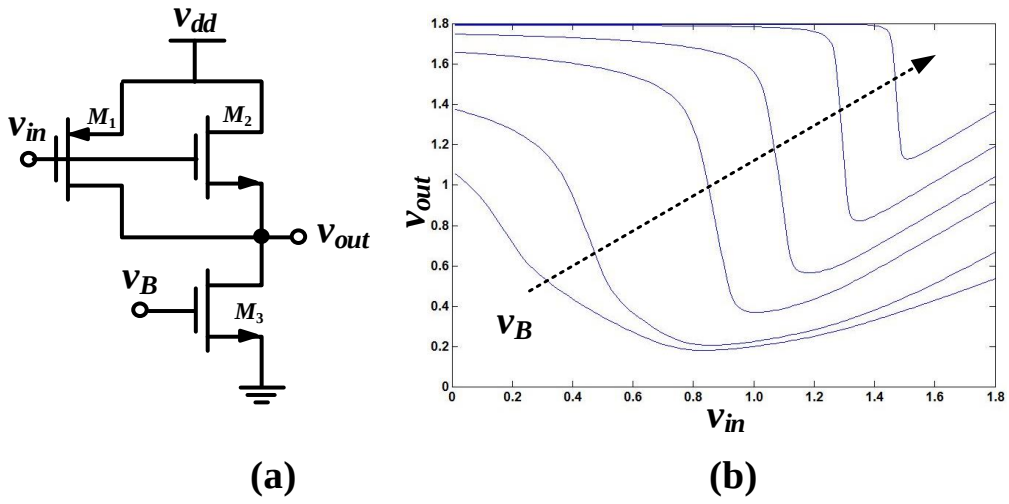

Figure 2.4 V-shape characteristic chaotic map (a) circuit and (b) transfer characteristic from various biasing voltage V_B.

2.2.1 Design and Implementation

A discrete-time chaotic oscillator circuit is designed using V-shape characteristic chaotic map circuit (inverse tent map). This map circuit designed using 3 transistors as illustrates in Figure 2.4 (a) and also the DC characteristic of chaotic map circuit with various biasing voltage between 0V to 1.8V is depicted in Figure 2.4 (b). Where M1 is operated in low voltage region, while M2 is operated when input of chaotic map circuit is greater than threshold voltage. Furthermore, the transfer characteristic of the proposed

chaotic map circuit can be modified by the adjusting of the bias voltage V_B at transistor M3.

In order to generate the chaotic signal, a two-phase clock is required to control overall process. On phase φ1 the chaotic map circuit was fed by value of x_n, through the transfer function $f(x_n)$, the output x_{n+1} is generated and then stored in capacitor C_1. On phase φ2 the stored value x_{n+1} is shifted through the buffer to capacitor C_2. Subsequently, the value is fed back into the input of chaotic map and all of process continues iteratively.

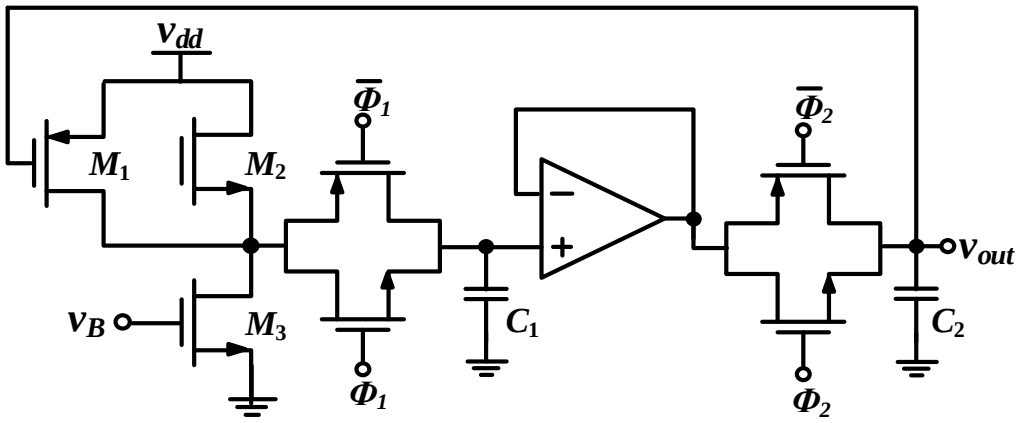

Figure 2.5 Circuit diagram of discrete-time chaotic Oscillator Circuit based on V-shape characteristic chaotic map.

2.2.2 Simulation Result

The discrete-time chaotic oscillator using approximation of V-shape characteristic chaotic map circuit is shown in Figure 2.5. The system was designed using Cadence and simulated using Hspice simulation with 0.18 µm CMOS technology. The system is supplied with 1.8V and clock 25 MHz to operate. The chaotic map circuit is made of transistors *M1*, *M2* and *M3* and the size of MOS transistors are 4/0.18 µm, 2/0.18 µm and 1.2/0.18 µm, respectively.

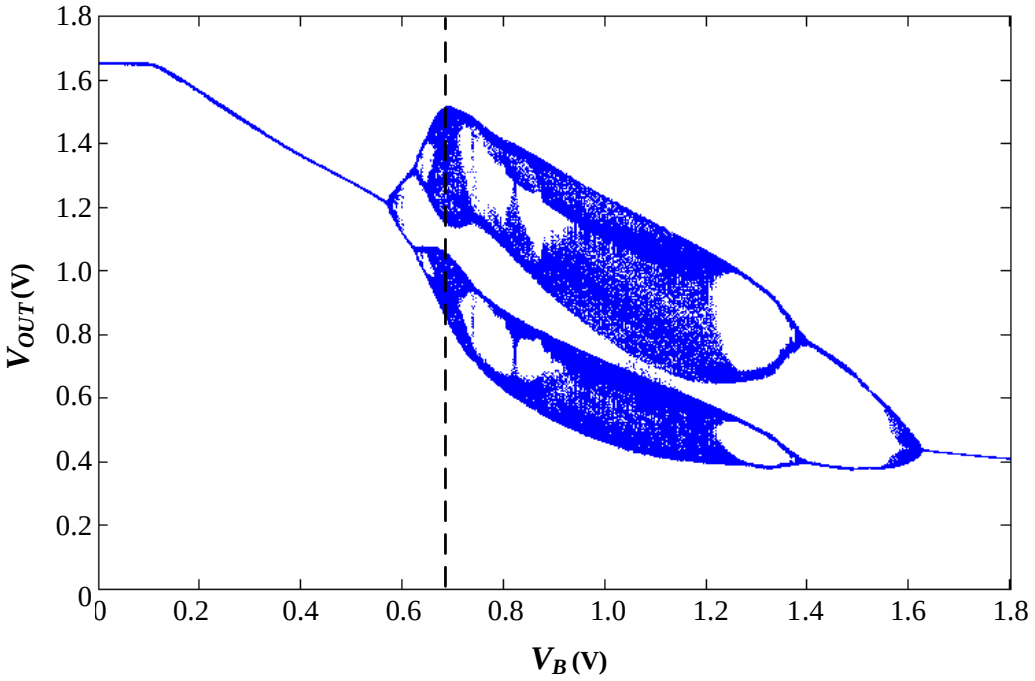

Figure 2.6 Plots of bifurcation diagram of the proposed chaotic oscillator circuit based on V-shape characteristic chaotic map.

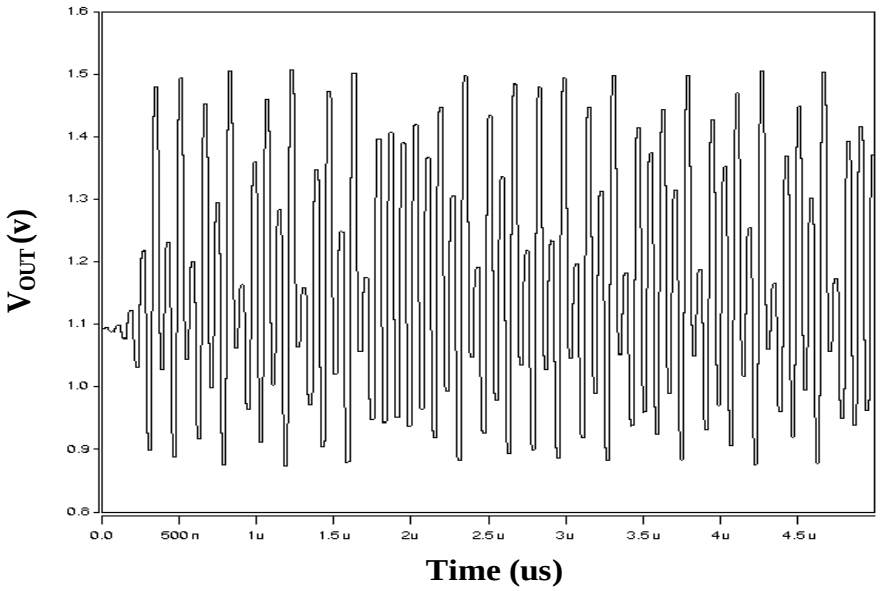

Figure 2.7 Transient waveforms for bias voltage V_B is 0.68V.

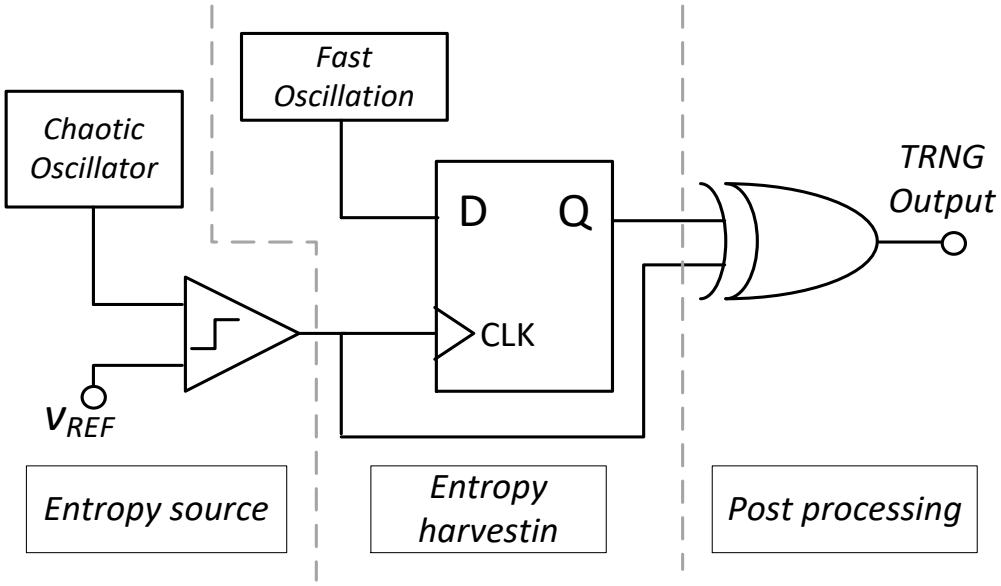

Figure 2.8 The proposed true random bit generator based on of chaotic oscillator with on V-shape characteristic chaotic map.

In order to examine the chaotic dynamics, Figure 2.6 depicts the plots of bifurcation diagram of the simulated chaotic oscillator circuit, obtained by plotting output signal samples when bias voltage (V_B) at transistor M3 was swept between 0V and 1.8V. The bifurcation can be simply to observed, white and blue regions in the diagram represent non-chaotic (windows of periodic behavior) and chaotic dynamics, respectively. It can be considered through the bifurcation diagram that the proposed chaotic oscillator circuit shows chaotic behaviors output. Figure 2.7 shows transient waveforms output of the circuit for the value of V_B at 0.68V which demonstrated non-periodic signal.

2.2.3 Dual Oscillator Sampling based True Random Bit Generator

Random bit generators are generally use in scientific and engineering. There are two principal methods used to generate random numbers. First, Pseudo Bit number

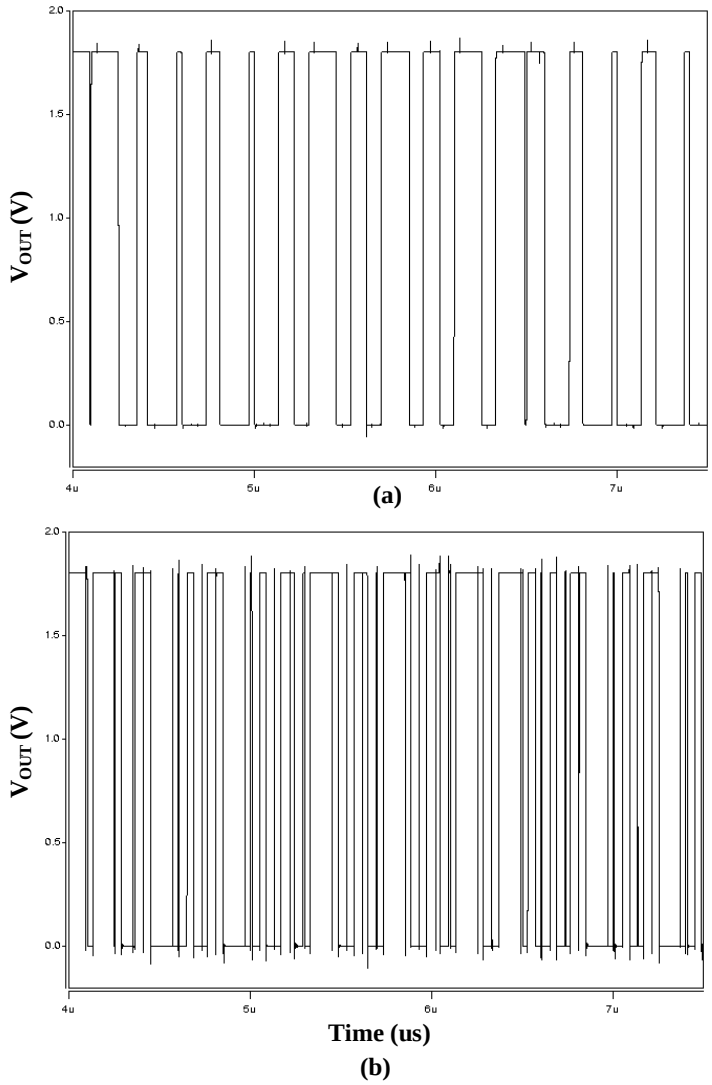

Figure 2.9 Output bit streams from generated from proposed true random bit generator; (a) before processing (b) after processing.

generator (PRBG) is based on deterministic algorithms, depending on an initial seed value. This type generator is vulnerable to observation and replication the output. On the other hand, True random bit generator (TRBG) is mainly based on physical source which is expected to be a randomness to generate random numbers sources such as nuclear decay, intrinsic topology imperfections, and thermal noise. The output bit sequences of a TRBG is expected to be unpredictable and statistically independent.

Typically, TRBG consists of three parts: entropy source, entropy harvesting mechanism and a post processing mechanism. From many literatures, the entropy sources have been described such as thermal noise, metastability stages of oscillator or chaotic oscillator. Various implementations of entropy source using chaotic oscillator. By reason of circuits can be designed where it has an extremely sensitivity to initial conditions and system parameters which cause it practically unpredictable the output. Entropy harvesting, is used to capture nondeterministic randomness from entropy sources. This is also a critical part which effect to quality of a TRBG. The random bit stream generated using an entropy harvesting mechanism may not fully robust for TRBG hence post-processing mechanism is required to improve quality.

In order to generate a true random signal, Figure 2.8 shown block diagram of true random bit generator using a combination of proposed discrete-time chaotic oscillator, dual oscillator sampling method [39] and Exclusive-OR gate (XOR), these components are used as an entropy source, entropy harvesting mechanism and post processing, respectively. The dual oscillator sampling method using a D flip-flop to exploits the association between two independent free running oscillators, a low frequency oscillator and high frequency oscillator. Output bits are generated where the output signal of a fast oscillator sampling at the rising edge of the slower clock. Subsequently, XOR gate was used. Two random bit streams from Chaotic Oscillator and D flip-flop are XORed to remove any correlation and increase the randomness of output and result the proposed TRBG to have a throughput of 23 Mbps. The output bit streams before and after the post processing is shown in Figure 2.9.

The true random bit generator was designed using chaotic oscillator as an entropy source of the generator which causes the system qualified as true random bit

generator. In addition, the dual oscillator sampling method and XOR were used to increase the randomness of output. The entire system was Cadence and simulated using Hspice simulation in 0.18μm CMOS technology using a simple and compact structure of circuit for the advantage in compatibility.

2.2.4 Randomness Performance Evaluation

According to the properties of a random sequence which can be described in terms of probability, the various statistical tests have been used to investigate the randomness of output sequence from random generator. This paper, the proposed true random bit generator was examined by NIST test suit

The NIST test suite issued by the National Institute of Standards and Technology which is a statistical test package consists of 15 tests and generally accepted as a standard test suit for any pseudo random bit generators (PRBG) or true random bit generators (TRBG). The test was use to examine the binary sequence by detected an existing pattern of value that indicates non-randomness of the sequences through the probability values (*P*-value). The p-value indicates a randomness of the generated binary sequences against perfect randomness hypothesis. It can be seen that generated binary sequences from the proposed TRBG pass all test methods in NIST test suit as shown in Table 2.3.

2.2.5 Conclusion

The design of V-shape characteristic chaotic map circuit using 3 transistors can be used properly as a nonlinear function of the discrete-time chaotic oscillator which exhibits a chaotic behavior. The oscillator was examined in terms of bifurcation diagram and output behaviors observation.

Table 2.3 Results of the NIST test suite

Test Methods	*P*-value	Results
Frequency (mono-bit)	0.527	Pass
Frequency Block	0.818	Pass
Runs	0.147	Pass
Longest Run of Ones Block	0.940	Pass
Binary Matrix Rank	0.291	Pass
Discrete Fourier Transform	0.745	Pass
Non-overlapping Template Matching	0.995	Pass
Overlapping Template Matching	0.898	Pass
Universal Statistical	0.245	Pass
Linear Complexity	0.548	Pass
Serial	0.777	Pass
Approximate Entropy	0.777	Pass
Cumulative Sums	0.973	Pass
Random Excursions	0.534	Pass
Random Excursions Variant	0.612	Pass

The proposed true random bit generator (TNRG) based on discrete-time chaotic oscillator has a throughput of 23 Mbps and evaluation the output signal through NIST tests suite which pass all the test. TRBG circuit was designed using Cadence in 0.18μm CMOS technology with 1.8 voltage supply and the simulation results was demonstrated through Hspice simulation. Furthermore, the TRBG offers a compact structure and high efficiency which suitable for many applications.

2.3 Discrete-Time Chaotic Oscillator: reverse sigmoid characteristic

2.3.1 Design and Implementation

Regarding to the previous section, the chaotic oscillator circuit can be designed using chaotic map with V-shape characteristic. In this section, discrete-time chaotic oscillator circuit based on a chaotic map with reverse sigmoid characteristic. The proposed chaotic map is designed using an inverter and a subtractor Op Amp. The proposed chaotic map and its transfer characteristic is shown in Figure 2.10 (a) and (b), respectively.

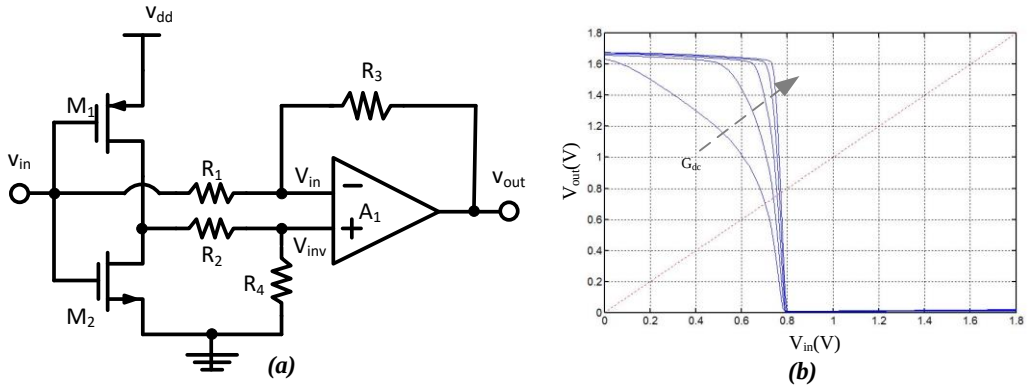

Figure 2.10 reverse sigmoid characteristic chaotic map (a) circuit and (b) transfer characteristic from various gain value G_{dc}.

Regarding to the proposed chaotic map, by setting $R_1 = R_2$, $R_3 = R_4$, the transfer function for subtractor circuit can be given by:

$$V_{out} = G_{dc}(V_{inv} - V_{in}) \tag{2}$$

where DC gain (G_{dc}) of circuit is defined as R_3 / R_1. The DC characteristic of the chaotic map circuit with various biasing voltage from 0 V to 1.8V is shown in Fig.2.10 (b) and It

can be seen that the characteristic can adjust by the value of G_{dc}.

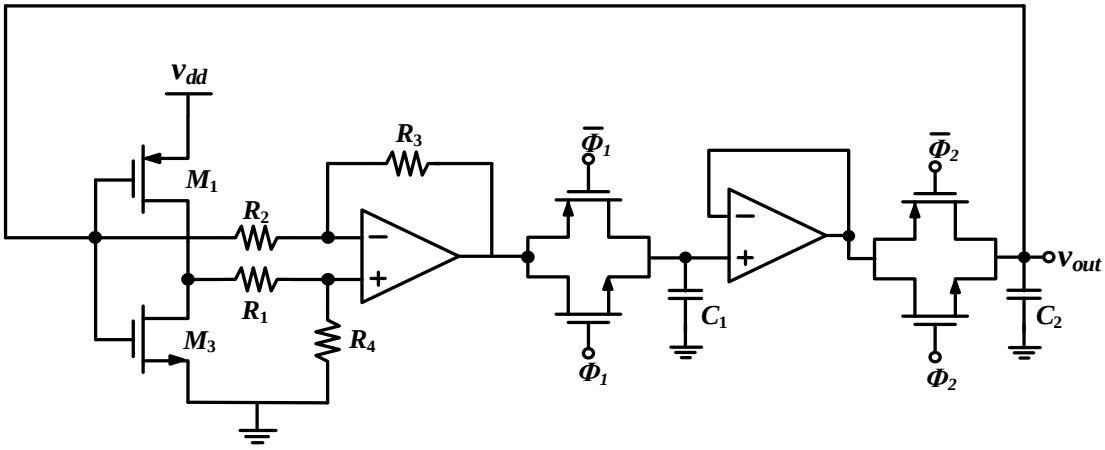

Figure 2.11 Circuit diagram of discrete-time chaotic oscillator circuit based on reverse sigmoid characteristic chaotic map.

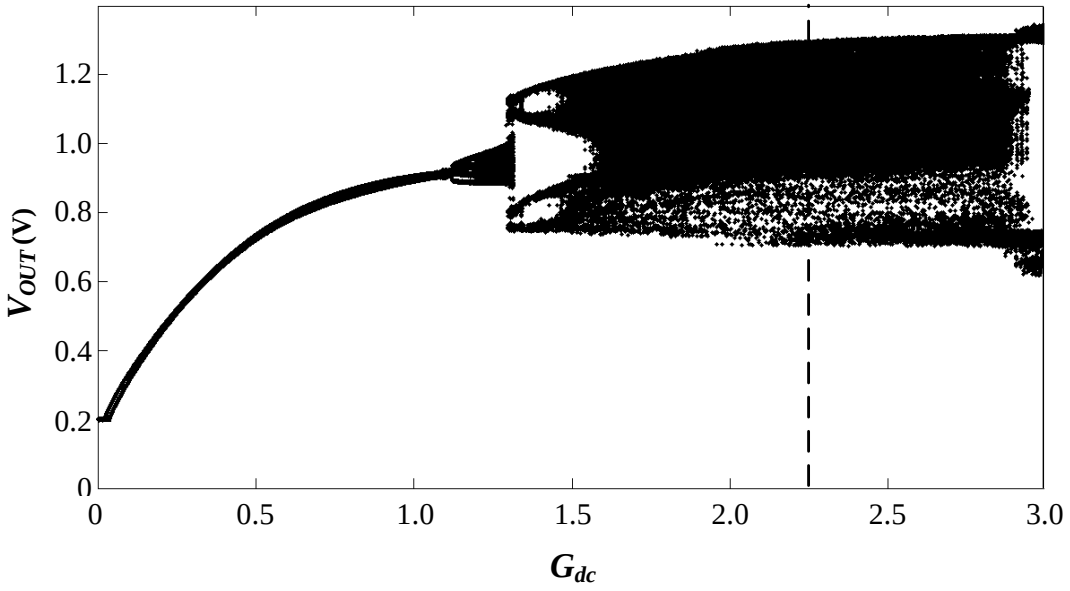

Figure 2.12 Plots of bifurcation diagram of the proposed chaotic Oscillator Circuit based on reverse sigmoid characteristic chaotic map.

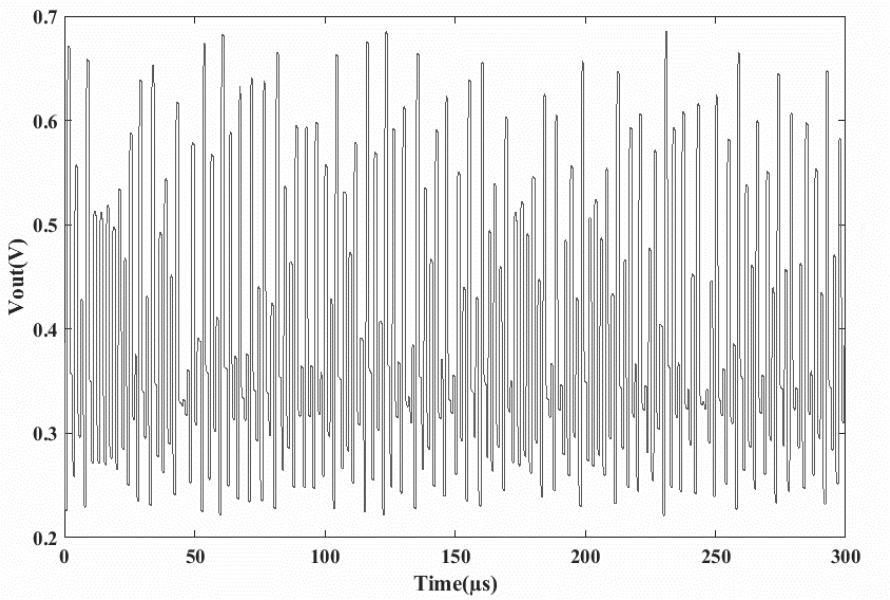

Figure 2.13 Transient waveforms of the proposed chaotic Oscillator Circuit based on reverse sigmoid characteristic chaotic map for the specific value of G_{dc} = 2.2.

2.3.2 Simulation Result

The proposed discrete-time chaotic oscillator circuit based on reverse sigmoid curve chaotic map was designed in Cadence and simulated HSPICE simulator while using 0.18 µm CMOS technology with 1.8 voltage supply. The size of the transistors used as inverter are as follow: M_1 = 4/0.18µm, M_2 = 2/0.18µm. The subtractor Op Amp circuit is same circuit as presented in Figure 2.3. The chaotic dynamics was examined by the plot of bifurcation diagram as depicted Figure 2.12. The plot of bifurcation diagram is obtained by plotting of the output signal from the simulated chaotic oscillator circuit where the value of gain G_{dc} vary between 0 to 3. The white region of the bifurcation represents nonchaotic behavior (periodic) while the black region represents the chaotic behavior (non-periodic). It can be considered through the bifurcation diagram that this proposed chaotic oscillator circuit based on reverse sigmoid curve chaotic map can offer a robust chaotic behavior. Figure 2.13 shows the transient simulation output of the circuit

for the value of G_{dc} = 2.2 and represents the complexity of chaotic behaviors.

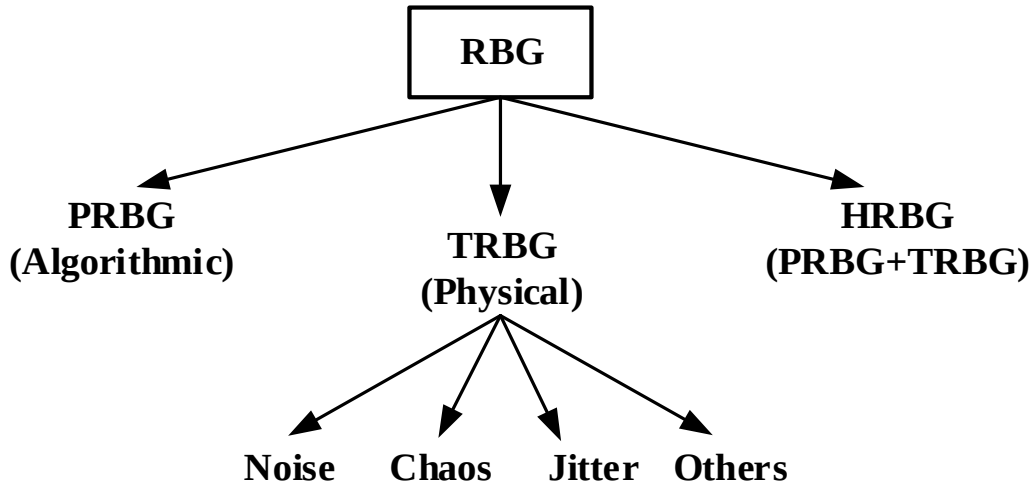

Figure 2.14 Classification of random bit generators

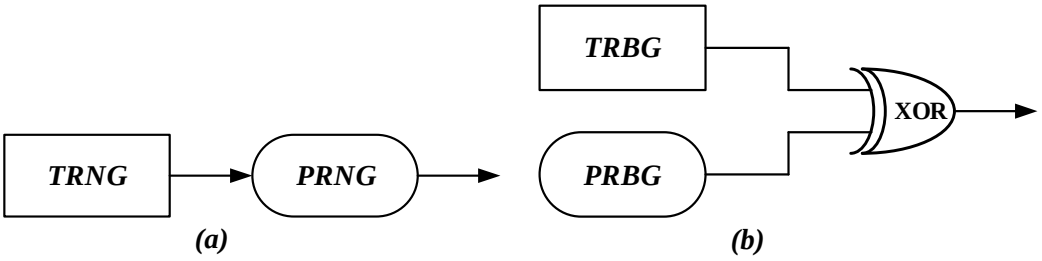

Figure 2.15 General structure of HRBG for both (a) series and (b) parallel connection

2.3.3 Hybrid Random Bit Generator

For decades of study, a countless of RBGs have been proposed. Typically, the statistical property of RBGs is relied on their randomness sources and most of the proposed RBGs can be classified into 2 types with respect to their randomness sources such a pseudo random bit generator (PRBG), a true random bit generator (TRBG). Though, lastly a combination of TRBG and PRBG as known as hybrid random bit generator (HRBG) was introduced [40-41]. This classification of RBG is shown in Figure

2.14. The PRBG is computational algorithms based random bit such as linear congruential generator or LFSR which also considered as deterministic RBG. On the other hand, TRBG is mostly based on the observation of some physical phenomenon that expected to be random such electrical noise, jitter, and chaotic which the output is completely unpredictable.

Hybrid random bit generator (HRBG) is a combination of TRBG and PRBG and typically, there are 2 types of connection as shown in Figure 2.15. First, The TRBG and PRBG can be connected in series as shown in Figure 2.15a by using the TRBG as a seed generator for PRBG which make the PRBG always produce an unpredictable output. Another approach is a parallel connection as shown in Figure 2.15b which can be done by XORing between the output of TRBG and PRBG.

According to mathematical statistics, the variance of linear combination of two sets of numbers is equal to the sum of the variances of each set as long as there is no correlation between the two sets. The linear combination of two sets of numbers can be done by adding, subtracting or XORing. This principle can be expressed as:

$$V_{XY} = V_X + V_y \tag{3}$$

In order to construct the HRBG, Figure 2.16 shows the block diagram of the proposed HRBG which is based on the combination of discrete-time chaotic oscillator based TRBG and LFSR using a parallel connection. Since the output of proposed TRBG is independent from PRBG, it can be assumed that the output of HRBG from XORing the output of TRBG and LFSR can provide a better statistical property than either the TRBG or the LFSR.

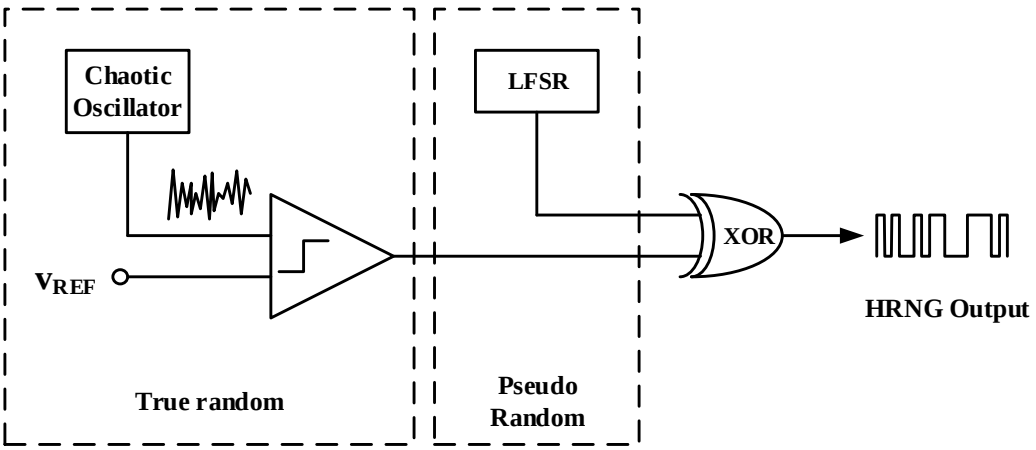

Figure 2.16 The Proposed HRBG based chaotic oscillator

2.3.4 Linear feedback shift register based Pseudo random bit generator

A linear feedback shift register (LFSR) is a chain of shift registers where the inputs are linear function of their previous state. In general, LFSR can be designed using exclusive-or (XOR) and flip-flop as a linear function and shift register. Each flip-flop output is connected to the next flip-flop input. The positions of shift registers, that output bit affected to the next stage, are called taps.

The initial value (also called the seed) is required for LFSR. The operation of register is deterministic with a finite number of possible states, which make the output of LFSR is determinable. Though the well-chosen feedback can make the LFSR produce all possible output values and this LFSR can be called maximal length LFSR.

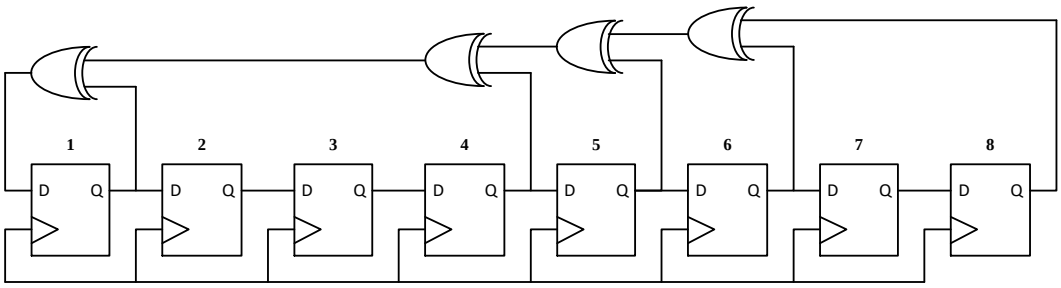

Figure 2.17 A Block Diagram of 8-bit Fibonacci LFSR

As the output of maximal length LFSR can typically pass all statistical tests, an 8-bit maximal length LFSR is implemented on MATLAB using Fibonacci structure where the taps are 8^{th}, 6^{th}, 5^{th} and 1^{st} as shown in Figure 2.17. The proposed LFSR is used to as a PRBG due to its deterministic output sequence.

2.3.5 Randomness Performance Evaluation

The random output of HRBG has been examined, according to the properties of a random sequence which can be described in terms of probability. Although the variety of statistical tests is existed, NIST test suit is the most widely used statistical test to investigate the randomness of output sequence from random bit generator.

The NIST test suite issued by the National Institute of Standards and Technology which is a statistical test package consists of 15 tests and generally accepted as a standard test suit for any random bit generators. The test can be used to examine the bit sequence by detected an existing pattern of value that indicates non-randomness of the sequences through the probability values (*P*-value) which is convenient in determining whether the random bit generator is suitable for cryptography or not. The *P*-value indicates a randomness of the test sequences where the *P*-value greater than 0.01, the sequence can be considered as random and accepted, otherwise rejected.

Table 2.4 shows the comparison of the results of NIST test suit from the raw bit sequence from the chaotic oscillator based random bit generator and the output sequence from the purposed HRBG. In this test, the raw bit sequence was generated from chaotic oscillator without any post processing method which can be seen that the raw bit sequence has failed many tests from NIST test result. Hence, the same NIST test suit was applied to output sequence from the purposed HRBG which was corrected from XOR operation

between the output of LFSR and chaotic oscillator based RNG. The statistically improvement of the result from the proposed HRBG can also be seen from NIST test result.

2.3.6 Conclusion

Traditionally, random bit generators (RBGs) are designed based on either physical phenomenon or computational algorithm as known as true random bit generator (TRBG) and pseudo random bit generator (PRBG), respectively. In this chapter a hybrid random number generator (HRBG) based on a combination of TRBG and PRBG was presented. A chaotic oscillator circuit was designed as a randomness source of TRBG using 0.18μm CMOS technology in Cadence software and simulated through HSPICE. An 8-bit LFSR as PRBG was designed in MATLAB software. The output of chaotic oscillator based TRBG and LFSR are XORed together to produce a random bit sequence. By such a simple structure, the proposed HRBG provides a throughput of 1 Mbps which has been statistically analyzed through NIST statistical tests suite and proved to be suitable for cryptography.

2.4 Conclusion and Discussion

In this chapter two discrete time chaotic oscillators have been presented. The first chaotic oscillator is a compact circuit based on chaotic map with only 3 transistors in order to achieve an approximate V-shape characteristic. The second proposed chaotic oscillator is based a chaotic map which is constructed in order achieve a reverse sigmoid characteristic. This chaotic oscillator may require a larger number of components though, the oscillator exhibits a robust chaotic behavior which can be seen from the plot of

bifurcation diagram. It can be seen from both transfer characteristic based chaotic oscillators that nonlinear functions with at least 1 turning point in transfer characteristic could induce chaos. Moreover, both chaotic oscillators show capability of using as a randomness source for the TRBGs and the output bit sequence is statistically analyzed through NIST tests suite which can pass all the test.

Table 2.4 Comparison of the results of the NIST test suite.

Test Methods	**Without HRBG**		**The Proposed HRBG**	
	***P*-value**	**Results**	***P*-value**	**Results**
Frequency (mono-bit)	x	Fail	0.964	Pass
Frequency Block	0.034	Pass	0.474	Pass
Runs	0.405	Pass	0.658	Pass
Longest Run of Ones Block	x	Fail	0.841	Pass
Binary Matrix Rank	0.421	Pass	0.291	Pass
Discrete Fourier Transform	0.013	Pass	0.218	Pass
Non-overlapping Template Matching	0.014	Pass	0.566	Pass
Overlapping Template Matching	0.637	Pass	0.898	Pass
Universal Statistical	0.057	Pass	0.537	Pass
Linear Complexity	0.451	Pass	0.868	Pass
Serial	0.097	Pass	0.785	Pass
Approximate Entropy	x	Fail	0.605	Pass
Cumulative Sums	x	Fail	0.462	Pass
Random Excursions	x	Fail	0.074	Pass
Random Excursions Variant	x	Fail	0.315	Pass

Chapter 3

Robustification of a One-Dimensional Generic Sigmoidal Chaotic Map with Application of True Random Bit Generation

This chapter presents the research and study regarding a 1-D sigmoidal chaotic map, which has never been distinctly investigated. In this chapter, a generic form of the sigmoidal chaotic map with three terms is introduced. The unification of modified sigmoid and hyperbolic tangent (tanh) functions reveals the existence of a "unified sigmoidal chaotic map" generically fulfilling the three terms, with robust chaos partially appearing in some parameter ranges. A simplified generic form through various S-shaped functions, has recently led to the possibility of linearization using (i) hardtanh and (ii) signum functions. This study finds a linearized sigmoidal chaotic map that potentially offers robust chaos over an entire range of parameters. Chaos dynamics are described in terms of chaotic waveforms, histogram, cobweb plots, fixed point, Jacobian, and a bifurcation structure diagram based on Lyapunov exponents. As a practical example, a true random bit generator using the linearized sigmoidal chaotic map is demonstrated. The resulting output is evaluated using the NIST SP800-22 test suite and TestU01.

3.1. Introduction

In 1993, Majumdar and Mitra [42] first coined the phrase "*robust chaos*" in dynamic optimization models represented by a quadratic map family. Later in 1996, a search for robust chaos in a discrete-time neural network was conducted by R. Dogaru et al. [43] to discover a compact set of parameters, included in a weight space, that could sustain chaotic behaviors but remain unchanged. In 1998, S. Banerjee et al. [44] defined robust chaos as "*the absence of periodic windows and coexisting attractors in some neighborhood of the parameter space.*" Such a definition implies that any changes or variations in system parameters would not result in the fragility of chaos. A practical example of robust chaos in a 2-D piecewise smooth system was also demonstrated through a current-mode controlled boost converter.

A search for robust chaos generation approaches has been of considerable interest due to the suitability of robust chaos in practical applications in science and engineering, such as cryptography and secure communications [45-50]. Andrecut and Ali [51,52] reconstructed 2-D smooth unimodal maps via non-integer powers for robust chaos by means of mapping a critical point into an unstable fixed point that was not in the basin of attraction of a periodic attractor where, consequently, no periodic attractors occurred. G. Perez [53] has further analyzed the linear interpolation between fully chaotic logistic and quartic maps suggested by S. Thomae, and the results reveal a bifurcation diagram without any periodic windows.

Recently, several approaches to the generation of robust chaos have been reported, involving techniques relating to (i) the determination of critical behavior of the Lyapunov exponent near the transition to robust chaos via type-III intermittency for a 1-

D singular map [54], (ii) two methods for a prescribed invariant measure and varying Lyapunov exponent as well as a prescribed constant invariant measure and varying Lyapunov exponent [55], (iii) a structural synthesis of a state space energy-based adaptive controller [56], (iv) the basis of symmetry violations in attractors [57], and (v) the invariant center manifold [58].

In 2012, the open problem on "*Is a unifying chaotic dynamic system possible?*" was raised by Z. Elhadj and J. C. Sprott [59], and a multifunction mathematical model, a so-called unified chaotic map, was proposed with the capability of generating hyperbolic, Lorenz-type, and quasi-attractors [60]. J.C. Sprott [61] also introduced a particular 2-D unified piecewise smooth map that contained Hénon and Lozi maps. It is remarkable to note that the unification of a piecewise smooth map could exhibit robust chaos in some portions of a bifurcation parameter region, which is, in fact, a transition between Hénon and Lozi maps.

In accordance with [60,61], it is natural to wonder whether there is a possibility of the unification of a category of simple 1-D smooth chaotic maps that can generate robust chaos. Exhaustive searches and investigations into a family of S-shaped functions have led to a generic form for a smooth sigmoidal chaotic map, presented in this paper. The unification and simplification of the generic smooth sigmoidal chaotic map will be discussed. The linearization of a simplified smooth sigmoidal chaotic map using either the hardtanh or the signum function potentially exhibits robust chaos over an entire range of parameters. Chaos dynamics will be described in terms of apparent time-domain chaotic waveforms and their histogram, cobweb plots, frequency spectrum, equilibria, Jacobian, bifurcation structure diagram based on Lyapunov exponents, bifurcation diagram, and recurrence plot (RP). As for practical examples, a true random bit generator (TRBG)

with statistical tests results from the NIST SP800-22 test suite and TestU01 using the linearized sigmoidal chaotic map will be demonstrated.

3.2. Generic One-Dimensional Sigmoidal Chaotic Maps

3.2.1 Unification of Generic Sigmoidal Chaotic Map

The proposed unification process commences by considering a generic sigmoidal chaotic map, which can be preliminarily defined by the recurrence relation of the form

$$x_{n+1} = \mp A f_{\mathrm{NL}}(Bx_n) \pm Cx_n \pm D \tag{3.1}$$

where x_n is a real variable, $f_{\mathrm{NL}}(x_n)$ is a sigmoidal function, and the parameters A, B, C, and D are real constants. With reference to (3.1), this paper initially considers a typical sigmoid function, which exhibits S-shaped transfer function characteristics within the range (0, 1) throughout an entire domain (-∞, +∞). In other words, a mathematical model is $f(x) = 1/(1 + \exp(-x))$. Nonetheless, the substitution of the sigmoid function as $f_{\mathrm{NL}}(x_n)$ in (3.1) could not induce chaos. Therefore, this paper realizes a modified sigmoid function $f_{\mathrm{mod}}(x)$ as follows:

$$f_{\mathrm{mod}}(x) = 2\left(\frac{1}{1+e^{-x}}\right) - 1 \tag{3.2}$$

It is seen in (3.2) that the range of $f_{\mathrm{ms}}(x)$ is a typical sigmoid function where the function is doubled and shifted down to be (−1, 1). Notice that the nonlinearity in (3.2) apparently associates to a hyperbolic tangent (tanh) function, i.e.,

$$f(x) = \tanh(x) = \frac{1-e^{-2x}}{1+e^{-2x}} = 2\left(\frac{1}{1+e^{-2x_n}}\right) - 1 \tag{3.3}$$

Note that the constant 2 is essential as a result of the mathematical transformation. Realizing functions (3.2) and (3.3) in the generic sigmoidal chaotic map results in a unified sigmoidal chaotic map that contains modified sigmoid and tanh functions given by

$$x_{n+1} = \pm 2\left(\frac{1}{1+e^{-Bx_n}}\right) \mp Cx_n \mp 1 \tag{3.4}$$

It is clear that Equation (3.4) provides three complete mathematical terms to the generic sigmoidal chaotic map described in (1), where parameters *A* and *D* are 2 and 1, respectively, while parameters *B* and *C* are assigned as bifurcation parameters. Equation (3.4) also comprises a conjugate of two unified sigmoidal chaotic maps as follows:

$$x_{n+1} = 2\left(\frac{1}{1+e^{-Bx_n}}\right) - Cx_n - 1 \tag{3.5}$$

$$x_{n+1} = -2\left(\frac{1}{1+e^{-Bx_n}}\right) - Cx_n + 1 \tag{3.6}$$

In order to investigate the chaotic dynamics of the unified sigmoidal chaotic maps, the Lyapunov exponent (LE) is calculated. The LE is defined as a quantitative measure that characterizes the rate of separation of infinitesimally close trajectories, and can be described as

$$\mathrm{LE} = \lim_{\mathrm{N}\to\infty} \frac{1}{\mathrm{N}} \sum_{n=1}^{\mathrm{N}} \log_2 \frac{\mathrm{d}x_{n+1}}{\mathrm{d}x_n} \tag{3.7}$$

where N is the number of iterations. A positive LE typically indicates chaotic behaviors, and a larger value of LE results in a higher degree of chaoticity. The LEs of the system are calculated by using 100,000 iterations of data. Figure 3.1 illustrates plots

of a bifurcation structure of parameters C versus B of the unified sigmoidal chaotic map in (3.5), where the heat diagram indicates a positive LE and a white color represents a non-chaotic region while the black color represents the maximum LE of 1. The shading means that the LE increases correspondingly from yellow to red. Within the region of parameters $0 < B < 100$ and $1 < C < 2$, the white color roughly indicates where LE ≤ 0, and it appears in a few regions. However, there is some partial portion of parameter space that appears to be robust.

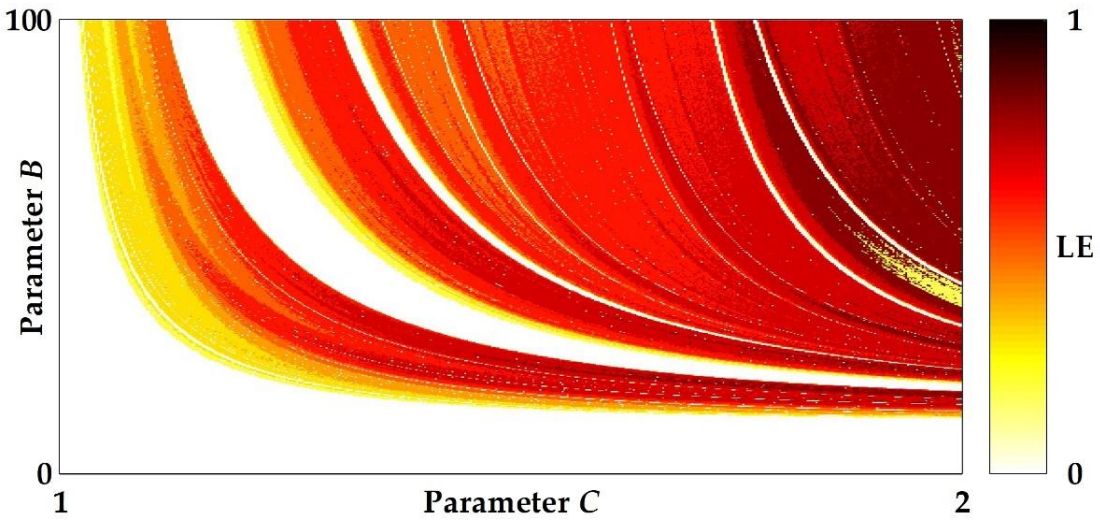

Figure 3.1. Plots of a bifurcation structure of parameters C versus B of the unified sigmoidal chaotic map in (3.5), where the heat diagram indicates a positive Lyapunov exponent.

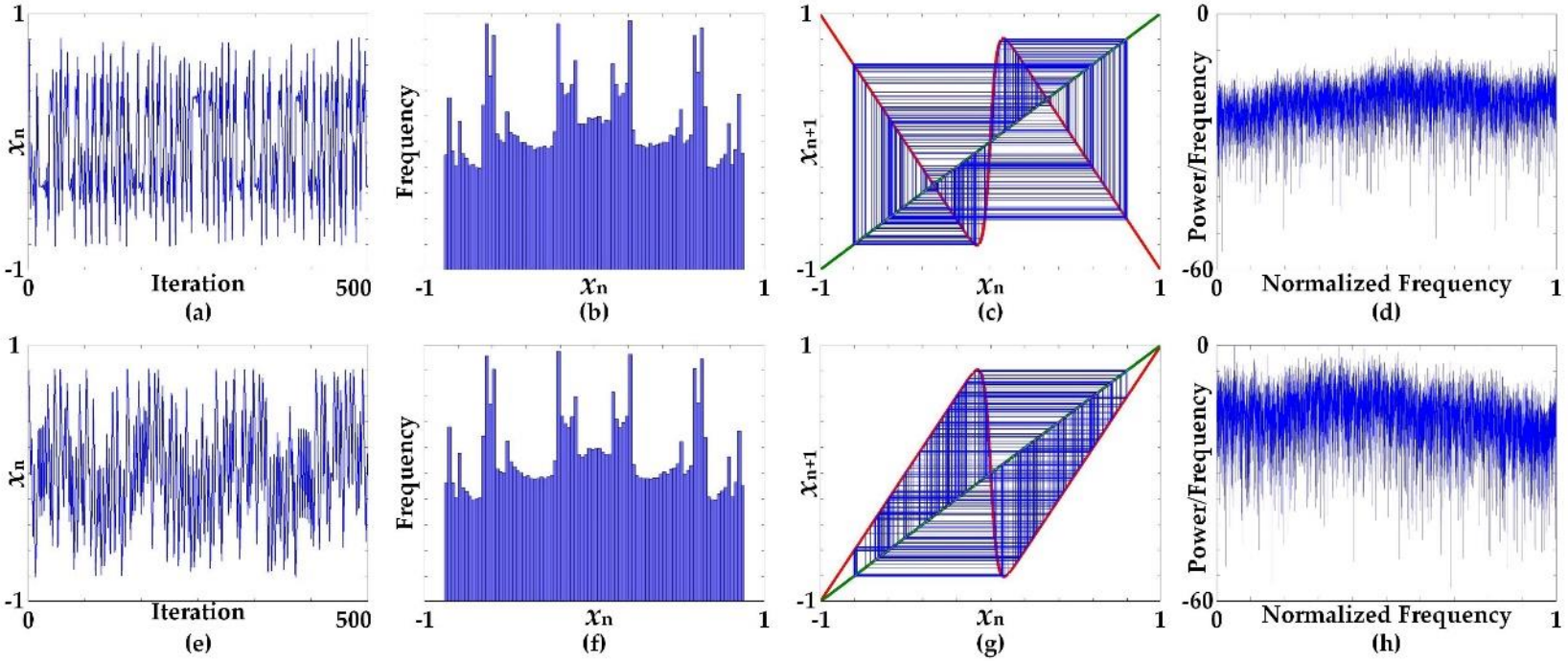

Figure 3.2. Characteristics of chaotic waveforms in time domain and plots of histogram, cobweb, and frequency spectrum using periodogram at specific parameters $B = 75$ and $C = 1.9$; (a–d) characteristics of Equation (5), (**e**–**h**) characteristics of Equation (3.6).

Figure 3.2 shows the characteristics of time-domain chaotic waveforms and the histogram, cobweb, and frequency spectrum using periodogram plots at specific parameters B = 75 and C = 1.9, arbitrarily selected from the chaotic region. The waveforms in the time domain are apparently chaotic but are slightly different. The histograms for both Equations (3.5) and (3.6), obtained from 100,000 iterations, are very similar. However, the characteristics of the cobweb plots are significantly different. Equation (3.5) exhibits a superimposed square pattern, while Equation (3.6) reveals a hexagon pattern. It can be seen from the frequency spectrum that both Equations (3.5) and (3.6) offer a flat spectrum feature.

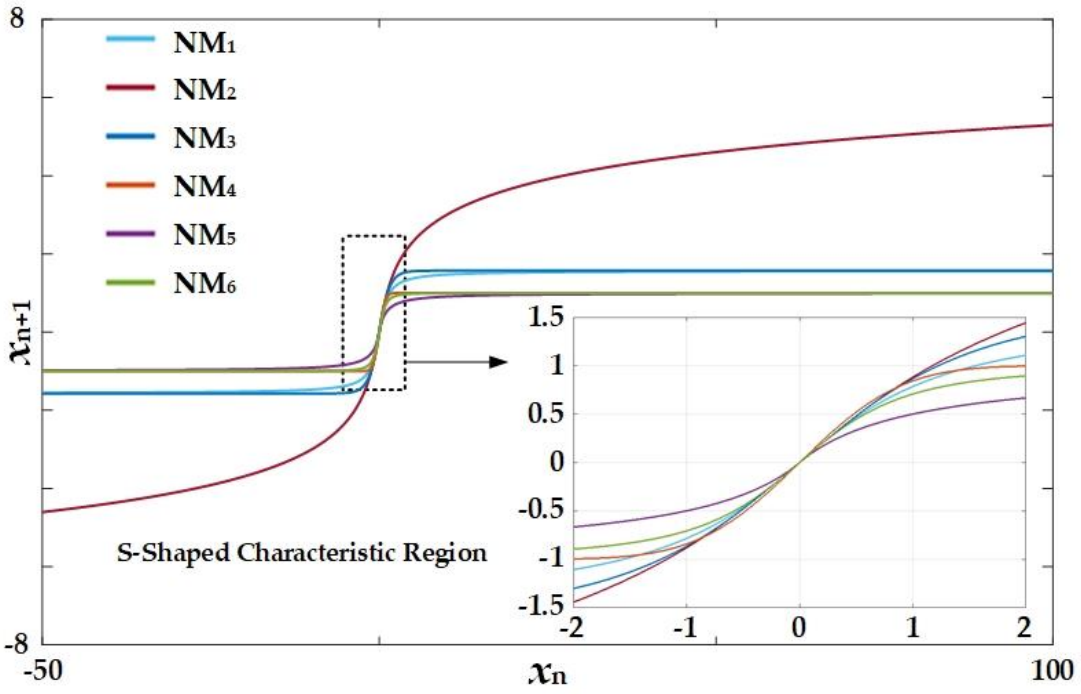

Figure 3.3. Plots of transfer function characteristics of the nonlinear functions of the cases NM_1 to NM_6.

3.2.2 Simplification of Generic Sigmoidal Chaotic Map

With reference to a generic sigmoidal chaotic map in (3.1), it is also possible to simplify a mathematical model through the utilization of other S-shaped nonlinear functions through the specific parameters $A = 1$ and $D = 0$. In other words, the simplified generic sigmoidal chaotic map is

$$x_{n+1} = \mp f_{\mathrm{NL}}(Bx_n) \pm Cx_n \tag{3.8}$$

Table 3.1 summarizes six simplified chaotic maps based on (3.8), the results of utilizing nonlinear functions $f_{\mathrm{NL}}(x)$ with S-shaped transfer function characteristics. With respect to the mathematical aspects, the cases NM_1, NM_2, and NM_3 are based on inverse trigonometric properties. Meanwhile, the case NM_4 is a special function in the form of an integral, which is originally derived from a Gaussian function, while NM_5 and NM_6 are special differentiable algebraic functions.

In order to investigate and compare S-shaped transfer function characteristics, Figure 3.3 depicts plots of transfer functions of the six nonlinear functions. It is apparent that only NM_4 has a range in the y-axis in the region (−1, 1), which closely resembles nonlinearity in a unified sigmoidal chaotic map, whereas the range of NM_2 appears to be $(-\infty, +\infty)$. The ranges of the four remaining cases are limited at certain specific levels. This phenomenon implies that the S-shaped nonlinearity that plays an important role in inducing chaos occurs in a short domain of approximately (−2, 2), and, therefore, the parameter *B*, which was introduced in the generic sigmoidal chaotic map, consequently becomes a significant factor in determining the chaos dynamics.

Table 3.1 Summary of six simplified sigmoidal chaotic maps involving nonlinear functions $f_{NL}(x)$ with S-shaped transfer function characteristics.

Cases	Descriptions	$f_{NL}(x)$ with No Parameters	Chaotic Maps
NM1	Inverse Tangent Function	$f_{NL1}(x) = \tan^{-1}(x)$	$x_{n+1} = \mp\tan^{-1}(Bx_n) \pm Cx_n$
NM2	Inverse Hyperbolic Sine Function	$f_{NL2}(x) = \sinh^{-1}(x)$	$x_{n+1} = \mp\sinh^{-1}(Bx_n) \pm Cx_n$
NM3	Gudermannian Function	$f_{NL3}(x) = \tan^{-1}(\sinh(x))$	$x_{n+1} = \mp\tan^{-1}(\sinh(Bx_n)) \pm Cx_n$
NM4	Error Function	$f_{NL4}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$	$x_{n+1} = \mp\frac{2}{\sqrt{\pi}}\int_0^{Bx} e^{-t^2}dt \pm Cx_n$
NM5	Soft Signum Function	$f_{NL5}(x) = \frac{x}{1+\lvert x\rvert}$	$x_{n+1} = \mp\frac{Bx_n}{1+\lvert Bx_n\rvert} \pm Cx_n$
NM6	Specific Algebraic Function	$f_{NL6}(x) = \frac{x}{\sqrt{1+x^2}}$	$x_{n+1} = \mp\frac{Bx_n}{\sqrt{1+(Bx_n)^2}} \pm Cx_n$

3.3 Linearization of Simplified Sigmoidal Chaotic Map for Robust Chaos

Regarding (3.8), rather than utilizing any S-shaped nonlinear functions, the linearized sigmoidal functions including the hardtanh and signum functions are employed. In other words, the proposed linearized sigmoidal chaotic maps are as follows:

$$x_{n+1} = \mp\text{hardtanh}(Bx_n) \pm Cx_n \tag{3.9}$$

$$x_{n+1} = \mp\text{sgn}(Bx_n) \pm Cx_n \tag{3.10}$$

where the hardtanh and signum are defined as

$$\text{hardtanh}\left(x\right)=\begin{cases}-1; & x<-1\\ x; & -1\le x\le 1\\ 1; & \text{x}>1\end{cases} \tag{3.11}$$

$$\text{sgn}\left(x\right)=\begin{cases}-1; & x<-1\\ 0; & x=0\\ 1; & \text{x}>1\end{cases}=\begin{cases}\dfrac{x}{|x|}; & x\neq 0\\ 0; & x=0\end{cases} \tag{3.12}$$

The linearized sigmoidal chaotic map based on the hardtanh function in (3.9) is a conjugate of two chaotic maps, i.e.,

$$x_{n+1}=\text{hardtanh}\left(Bx_n\right)-Cx_n \tag{3.13}$$

$$x_{n+1}=-\text{hardtanh}\left(Bx_n\right)+Cx_n \tag{3.14}$$

Meanwhile, the linearized sigmoidal chaotic map for (3.10), based on the signum function, is also the conjugate of two chaotic maps and can be expressed as

$$x_{n+1}=\text{sgn}\left(Bx_n\right)-Cx_n \tag{3.15}$$

$$x_{n+1}=-\text{sgn}\left(Bx_n\right)+Cx_n \tag{3.16}$$

In order to investigate the chaotic dynamic of the linearized sigmoidal chaotic maps, the Jacobian of the linearized sigmoidal chaotic map, which can be calculated through a first derivative as $|J(x_n)| = f'(x_n)$, is considered. Typically, the discrete time system becomes unstable in the condition of $|J(x_n)| > 1$, while the chaotic map needs to operate under an unstable condition in order to induce the chaos. With reference to (3.9), the unstable region of the linearized sigmoidal chaotic maps based on the hardtanh function, which is the parameter region where the chaos can occur, is calculated and

provides the following result,

$$|C| > 1 \cup |C - B| > 1 \tag{3.17}$$

whereas the unstable region of the linearized sigmoidal chaotic maps based on the signum function in (3.10) is calculated and results in

$$|C| > 1 \tag{3.18}$$

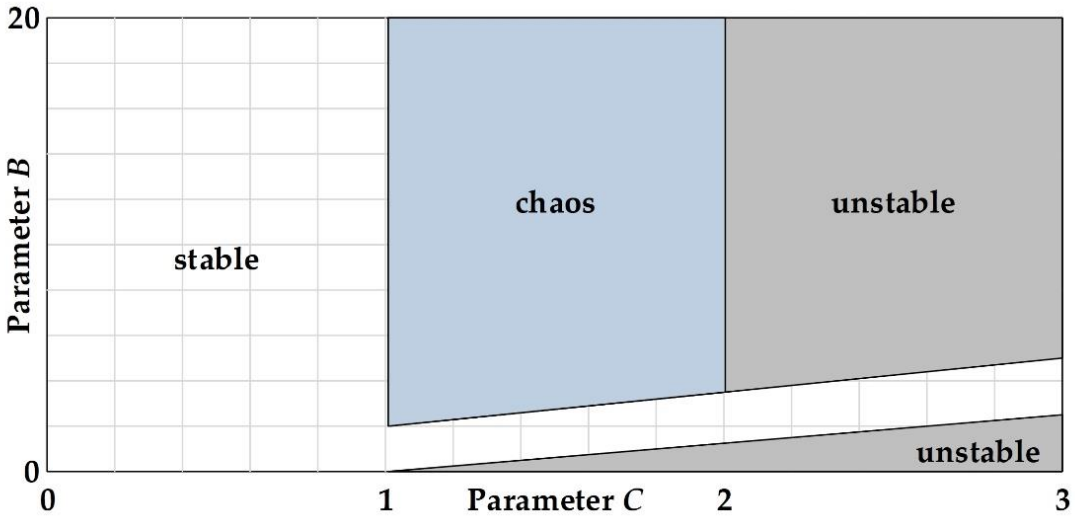

Figure 3.4. The plots of unstable and chaos regions with reference to (3.17), where the regions in grey and blue represent the unstable region and the chaos region, respectively.

Within the region of parameters $0 < B < 15$ and $1 < C < 3$, Figure 4 depicts the plots of the unstable and chaos regions, where the grey region represents the unstable region regarding (3.17), while the chaos region, which is considered a subset of the unstable region, is represented by the blue region. The chaos region in Figure 3.4 corresponds to the plots of the bifurcation structure of parameters *C* versus *B* with regard to the linearized sigmoidal chaotic maps based on the hardtanh function in (3.13), as shown in Figure 3.5. Nonetheless, the plots of the bifurcation structure of parameters *C*

versus *B* for the linearized sigmoidal chaotic map based on the signum function in (3.15), which is illustrated in Figure 3.6, shows the exact same values of LE for any values of *B* with respect to the signum function in (3.12). It is noticeable that the bifurcation structure in Figures 3.5 and 3.6 illustrate the results according to the unstable regions in (3.17) and (3.18), respectively.

The chaotic map, considered the system $x_{n+1} = f(x_n)$, typically has a point where $x^* = f(x^*)$ and is considered a fixed point (equilibrium). Table 3.2 summarizes the fixed points of the linearized sigmoidal chaotic maps based on the hardtanh function in (3.13) and (3.14) and the signum function in (3.15) and (3.16), all of which appear to have three fixed points.

Table 3.2 Summary of the fixed points of the linearized sigmoidal chaotic maps.

Chaotic Map Equations	$x^* = f(x^*)$	**Fixed Points** x^*
(3.10)	$x^* = \text{hardtanh}(Bx^*) - Cx^*$	$0, \frac{1}{C-1}$ **and** $-\frac{1}{C-1}$
(3.11)	$x^* = -\text{hardtanh}(Bx^*) + Cx^*$	$0, \frac{1}{C+1}$ **and** $-\frac{1}{C+1}$
(3.12)	$x^* = \text{sgn}(Bx^*) - Cx^*$	$0, \frac{1}{C-1}$ **and** $-\frac{1}{C-1}$
(3.13)	$x^* = -\text{sgn}(Bx^*) + Cx^*$	$0, \frac{1}{C+1}$ **and** $-\frac{1}{C+1}$

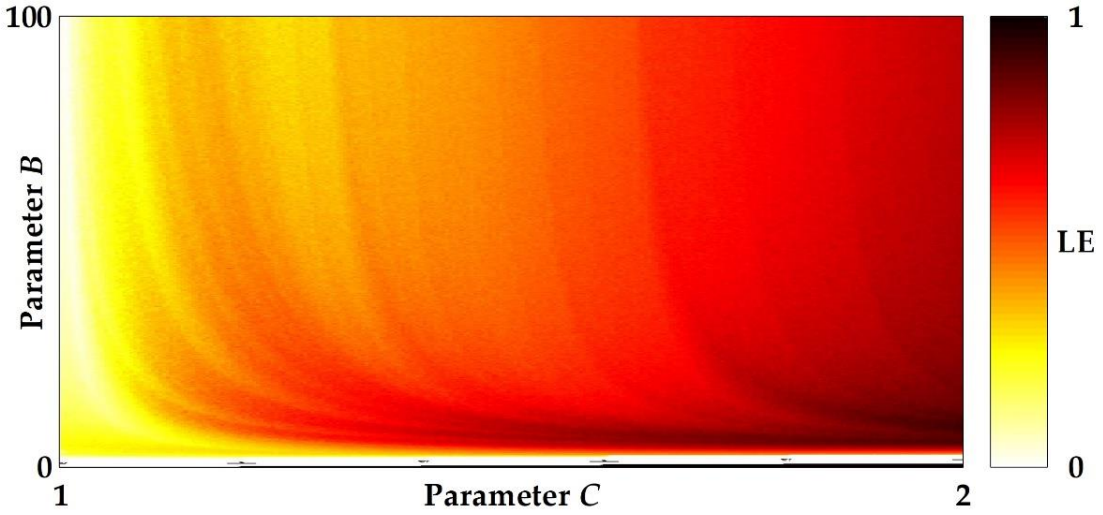

Figure 3.5. Plots of a bifurcation structure of parameter *C* versus *B* of the hardtanh-based linearized sigmoidal chaotic map in (3.13), where the heat diagram indicates a positive Lyapunov exponent.

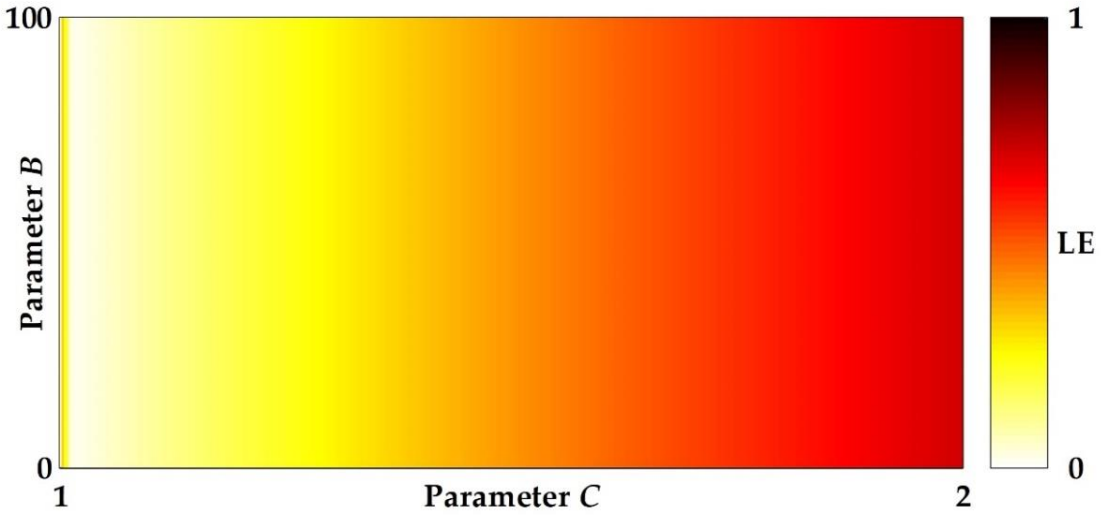

Figure 3.6. Plots of a bifurcation structure of parameters *C* versus *B* of the signum-based linearized sigmoidal chaotic map in (3.15), where the heat diagram indicates a positive Lyapunov exponent.

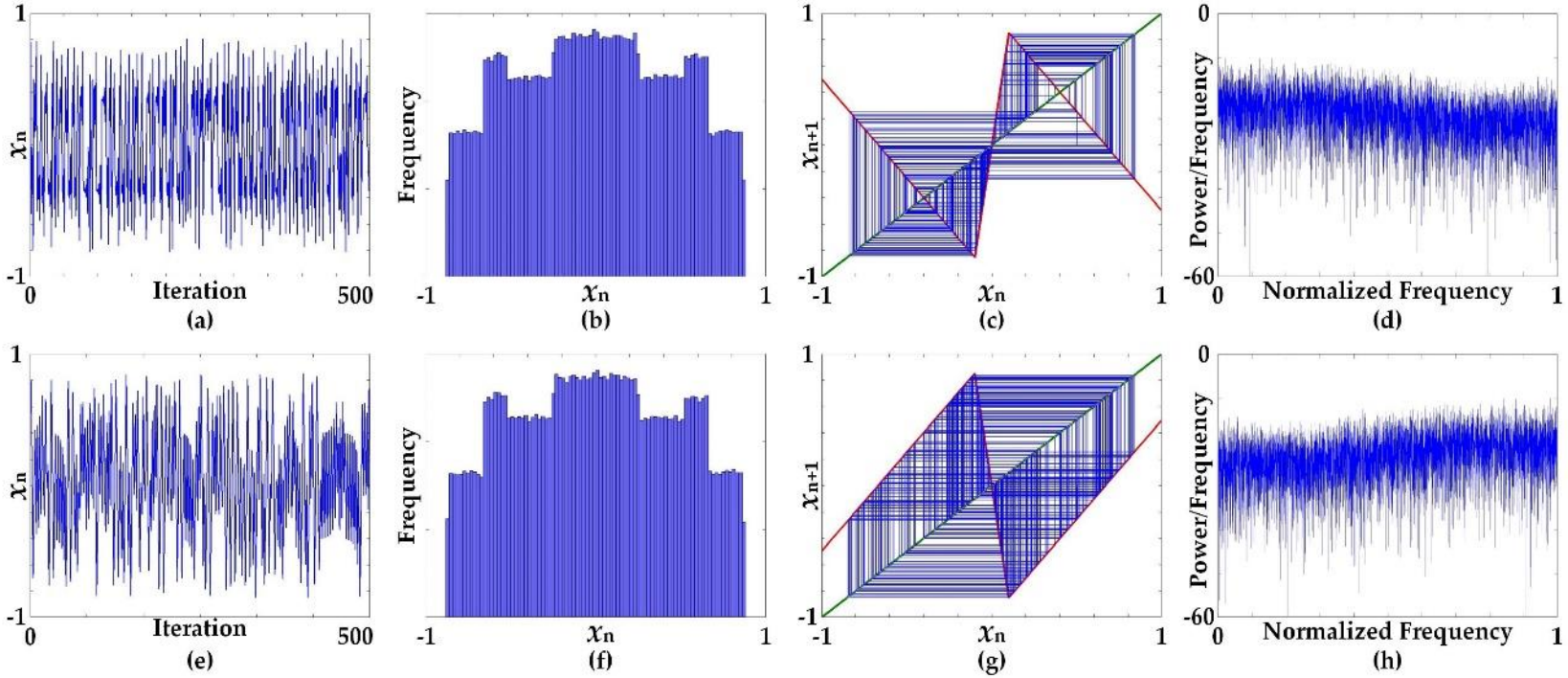

Figure 3.7. Characteristics of chaotic waveforms in time domain and plots of histogram, cobweb, and frequency spectrum using periodogram at specific parameters B = 15 and C = 1.9; (a–d) characteristics of Equation (3.13), (e–h) characteristics of Equation (3.14).

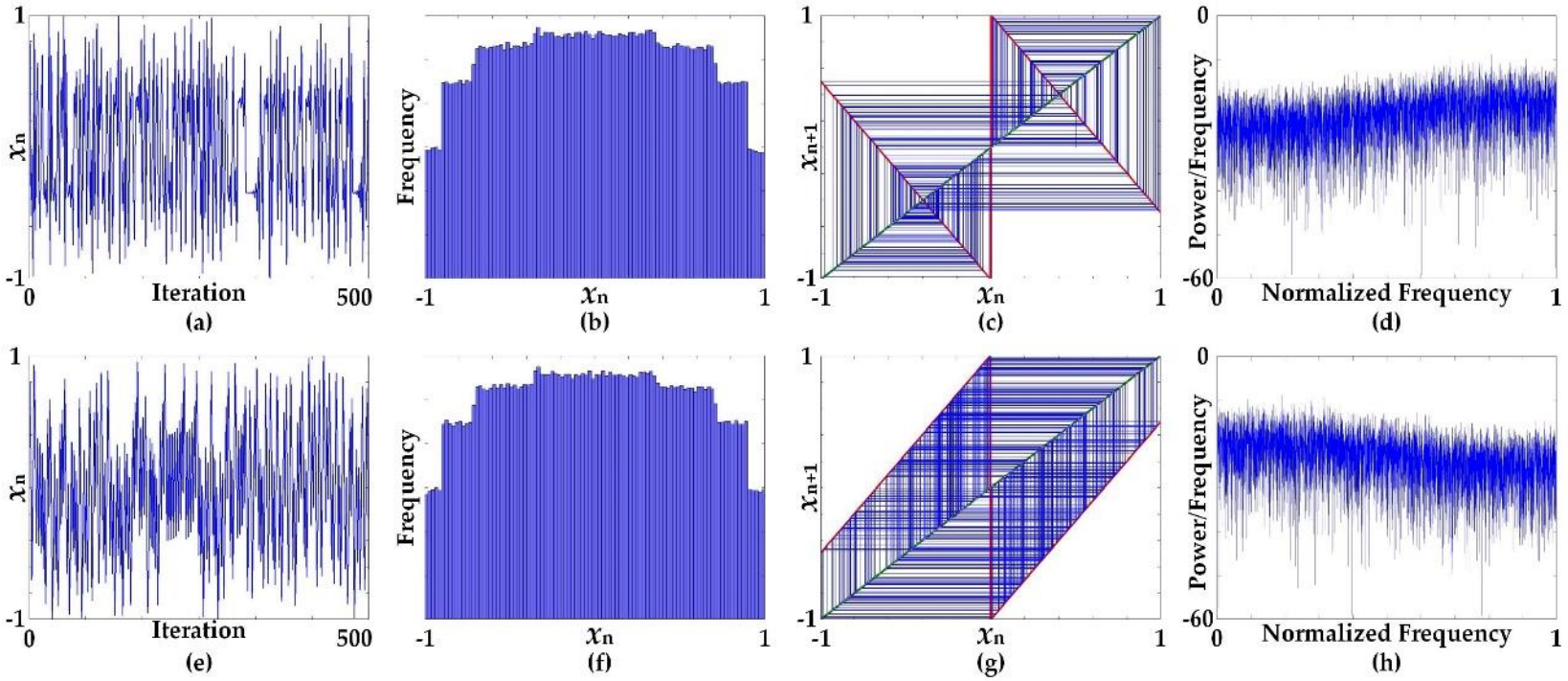

Figure 3.8. Characteristics of chaotic waveforms in time domain and plots of histogram, cobweb, and frequency spectrum using periodogram at specific parameter $B = 1$ and $C = 1.9$; (a–d) characteristics of Equation (3.15), (**e**–**h**) characteristics of Equation (3.16).

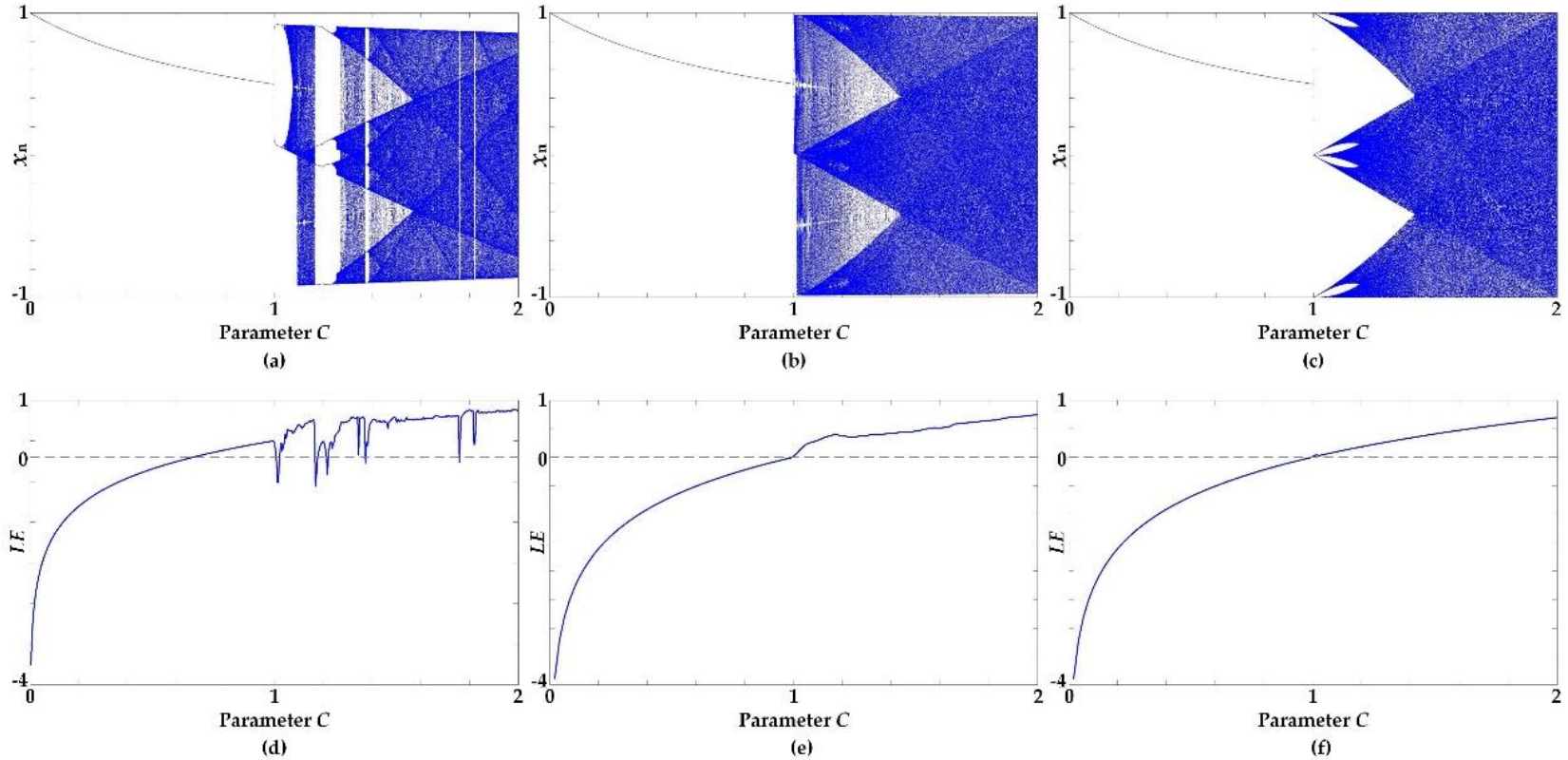

Figure 3.9. Plots of Bifurcation diagram and Lyapunov exponents (LEs) of chaotic maps at specific parameter $B = 75$; (a,d) the unified sigmoidal chaotic map in (3.5), (b,e) the hardtanh-based linearized sigmoidal chaotic map in (3.13), (c,f) signum-based linearized sigmoidal chaotic map in (3.15).

Figures 3.7 and 3.8 show the characteristics of the chaotic waveforms in the time domain as well as the histogram and cobweb plots at specific parameters, which were arbitrarily selected with regard to the chaotic regime, as seen in the bifurcation structure in Figures 3.5 and 3.6. The characteristics of the cobweb plots are associated with the fixed points of the chaotic maps, as shown in Table 3.2 In the case where the fixed point is 0, it is a globally asymptotically stable point, as in $|J(0)| = 0$. The stability of the fixed point appears in the cobweb plot, where the inward spiral corresponds to the attraction of the stable fixed point, while the outward spiral corresponds to the repelling of the unstable fixed point. The complex closed loops in the cobweb represent a high period of orbit, which indicates an infinite number of non-repeating values. The cobweb plots also relate to the boundary values of x_{n+1}, which depend upon the nonlinear term of the chaotic map, and for both cases of the linearized sigmoidal chaotic map in (3.9) and (3.10), the values of x_{n+1} fall into the region $(-1, 1)$.

The linearized sigmoidal chaotic maps based on the hardtanh function offer robust chaos over the entire range of parameters where $B > 3$ and $1 < C < 2$, while the linearized sigmoidal chaotic map based on the signum function shows robust chaos over the entire range of parameters where $1 < C < 2$.

Other than the proposed measurement tool, the bifurcation diagram is employed as a tool for a qualitative measure. A plots bifurcation diagram and LEs were used to identify the chaotic behavior as well as the continuity of the proposed chaotic maps as shown in Figure 3.9. While parameter C is considered a bifurcation parameter, the bifurcation diagrams of the linearized sigmoidal chaotic maps in (3.13) and (3.15), as shown in Figure 3.9b–c, illustrate chaotic behavior over the entire range of parameters where $1 < C < 2$, which corresponded to the LEs in Figure 3.9e–f. In other words, the

linearized sigmoidal chaotic maps can offer robust chaos over the entire range of parameters. Conversely, the bifurcation diagrams and the LEs of the unified sigmoidal chaotic maps in (3.5) as shown in Figure 3.9a appear to have some periodic windows and illustrate intermittently chaotic behavior, which means the unified sigmoidal chaotic maps can only offer robust chaos for some partial portion of the parameter.

The chaotic dynamics of the chaotic maps can also be described through a recurrence plot (RP) [62], as a typical random time series exhibits the RP with no structure while a periodic system causes the RP to exhibit some pattern. Figure 3.10 shows the RPs of the signum-based linearized sigmoidal for two different dynamic regimes. The purpose of the RP is to visualize the behavior of trajectories in phase space through a two-dimensional plot, which is especially beneficial in the case of high-dimensional systems. A dynamic system is represented by the trajectory ($\vec{x}_i$) in *d*-dimensional phase space; hence, the recurrence plot, which can be viewed as the recurrence of a state at time *i* at a different time *j*, is defined by the matrix

$$\mathrm{R}_{i,j} = \Theta\left(\varepsilon - \left\| \vec{x}_i - \vec{x}_j \right\| \right), \quad i, j = 1, \ldots, N, \tag{3.19}$$

where $\Theta(\cdot)$ is the Heaviside function, *N* is the number of points $\vec{x}_i$, and ε is a threshold. Figure 3.10a illustrates the RP which appear to be a dot pattern as a result the system that operated in the periodic regime, while Figure 3.10b illustrates the RP while the system is operated in the chaotic regime which results in a RP with no structure.

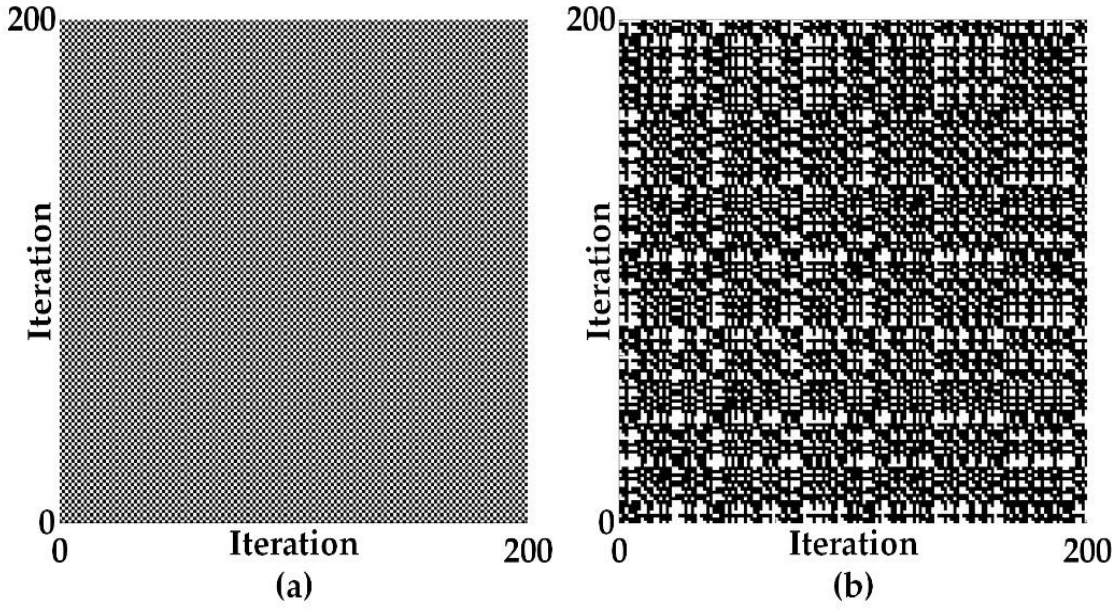

Figure 3.10. Recurrence plots of the signum-based linearized sigmoidal chaotic map in (3.15) for two different dynamic regimes, at specific parameter $B = 1$; (a) periodic regime: parameter $C = 0.5$, (b) chaotic regime: parameter $C = 1.9$.

3.4. True Random Bit Generation Based on the Linearized Sigmoidal Chaotic Map

The proposed true random bit generator (TRBG) is designed with respect to the typical structure of a true random bit generator, which consists of an entropy source, an entropy harvester, and a post-processor, as shown in Figure 3.11. The linearized sigmoidal chaotic map based on the signum function, which is driven by a sample and hold, is employed as the entropy source, and a comparator that acts as a 1-bit analog to the digital converter is considered the entropy harvester, while a quasi-shift register (QSR) is selected as the post-processor.

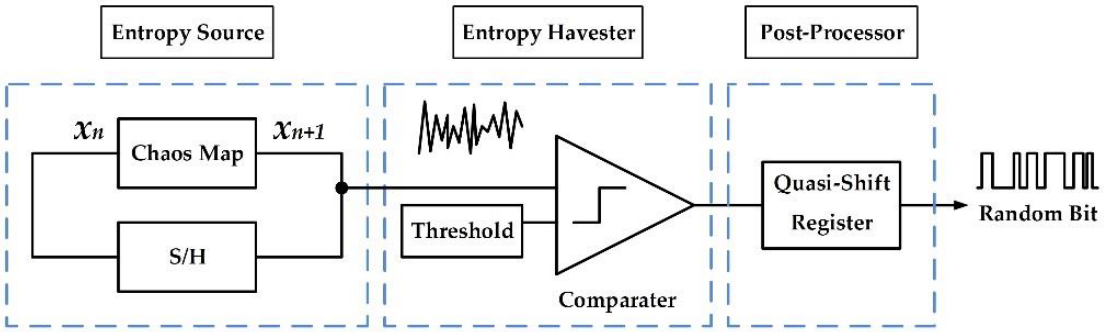

Figure 3.11. Proposed true random bit generator based on the signum-based linearized sigmoidal chaotic map.

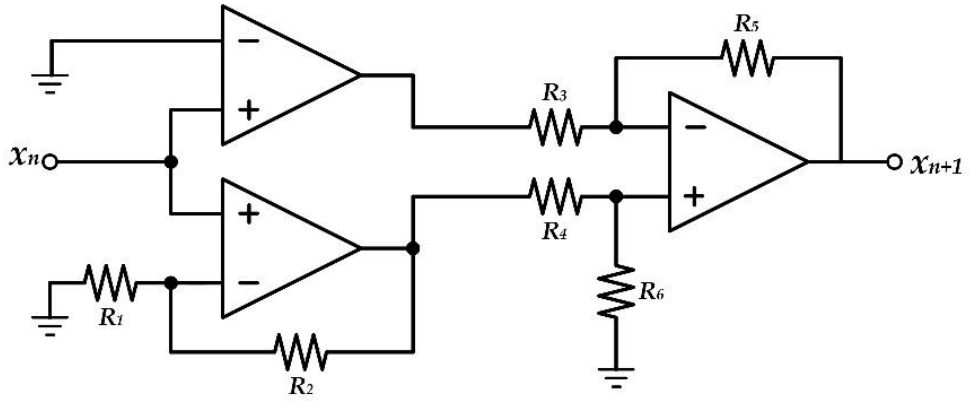

Figure 3.12. Circuit realizing the chaotic map with reference to the signum-based linearized sigmoidal chaotic map in (3.15).

3.4.1 True Random Bit Generator: Entropy Source

Theoretically, a chaotic map is deterministic, which means that if the initial condition of a chaotic map is exactly known, the output behavior can be exactly predicted. However, chaotic maps in practical implementation operate without the initial condition by inherent noise of the system and are amplified in the positive gain feedback loop by the iteration of the output signal in the map function. The output of the chaotic map will be unpredictable and suitable for true random bit generation.

A chaotic map can typically be considered as an entropy source of true random bit generation [63-65] though the robustness of the chaotic map is a concern. The robust chaos means the absence of a periodic window, and the existence of the periodic windows in the range of parameters of the chaos region implies that a small variation of the parameters would remove the system from the chaotic regime and discontinue the chaotic behavior [66].

Figure 3.12 shows the designed circuit of the chaotic map as the entropy source of the proposed TRBG, with reference to the signum-based linearized sigmoidal chaotic map in (3.15). The circuit consists of three operational amplifiers, (i) a comparator, (ii) a non-inverting operational amplifier, and (iii) a differential amplifier. The comparator operational amplifier is employed as the signum function, and it can be defined as

$$\mathrm{comp}(\mathrm{V}+) = \begin{cases} +\mathrm{V}cc; & \mathrm{V}+ > \mathrm{V}- \\ -\mathrm{V}cc; & \mathrm{V}+ < \mathrm{V}- \end{cases} \tag{3.20}$$

where V+ and V− are the inverting and non-inverting input of the comparator, respectively. The V+ can be considered an input x_n of the signum function, as a result of specifying the V−, which is a reference voltage of the comparator, as 0. In order for the comparator to perform as the signum function, the circuit is supplied with +1V and −1V as +V*cc* and –V*cc*, respectively.

Regarding the chaotic map in (3.15), the input x_n is amplified by the non-inverting operational amplifier gain, as $V_{out} = V_{in}(1 + R_2/R_1)$, where R_3, R_4, R_5, and R_6 are set to be equal. The subtraction of the output of the comparator from the amplified input ax_n results in the output of the chaotic map, x_{n+1}.

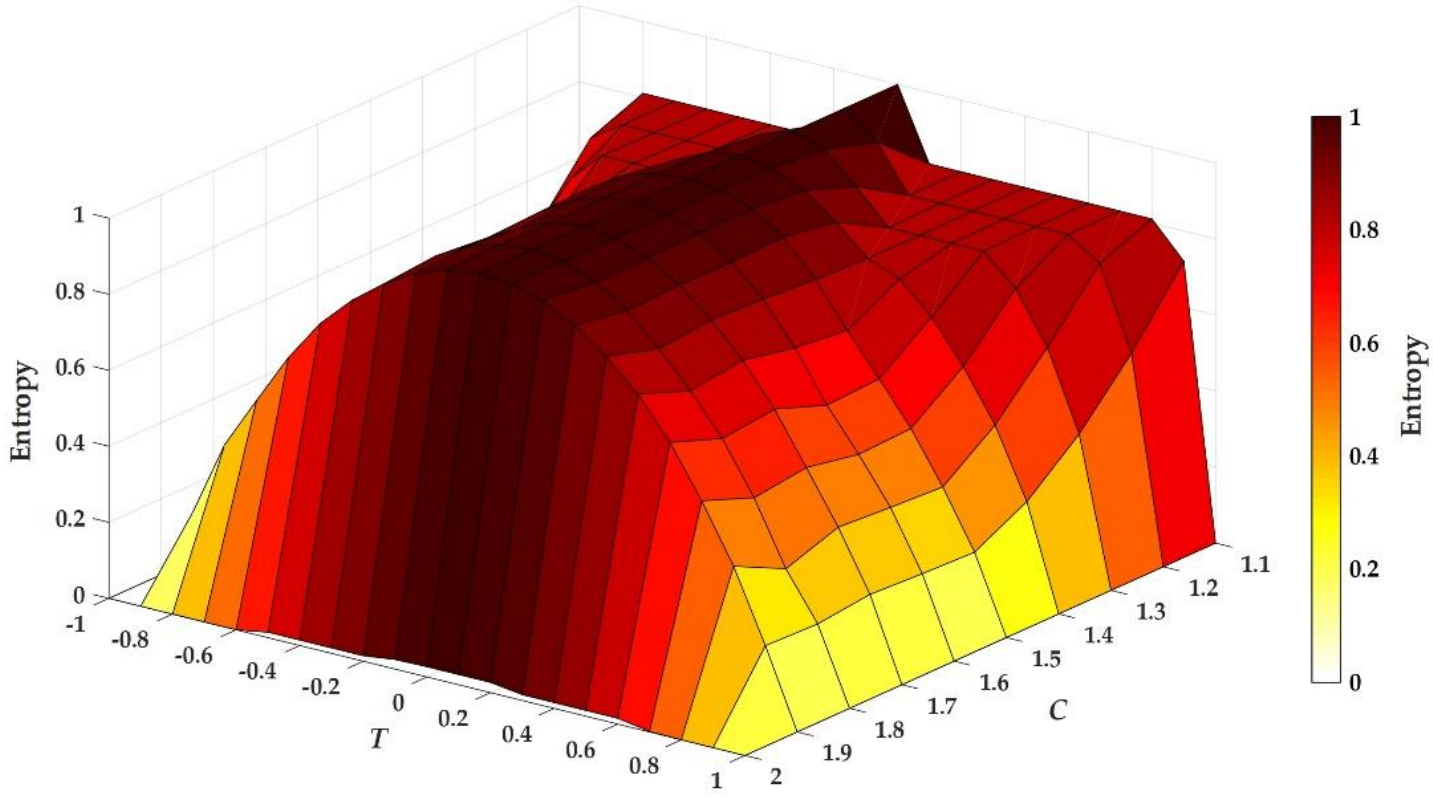

Figure 3.13. Plots of entropy versus threshold T and parameter C of the signum-based linearized sigmoidal chaotic map in (3.15).

3.4.2 True Random Bit Generator: Entropy Harvester

The comparator with threshold *T*, which is the entropy harvester, as shown Figure 3.11, digitizes the generated signal from the chaotic map; this can be expressed mathematically as

$$\mathrm{com}(x) = \begin{cases} 0; & x \le T \\ 1; & T \le x \end{cases} \tag{3.21}$$

The threshold is carefully chosen in order to generate numbers with a high level of randomness, or in other words, to harvest the entropy where it is at its maximum. Shannon's entropy is defined as

$$H = -\sum_{i=0}^{1} P_i \log_2 P_i \tag{3.22}$$

The entropy is calculated over the entire range of parameters, where $1 < C < 2$, resulting in the three-dimensional plot in Figure 3.13. The entropy is plotted versus the threshold value and parameter *C* of the signum-based linearized sigmoidal chaotic map in (3.15); note that the maximum entropy can be achieved when the threshold value is at 0 for any value parameter *C* in the chaotic regime.

3.4.3 True Random Bit Generator: Post-Processor

Even though the result from the entropy harvester is a random bit sequence, the post-processor is still required to improve the statistical imperfections of the generated sequences. Although there are many post-processing methods, the quasi-shift register was selected as the post-processor in the proposed TRBG due to its simple structure [67], with only a single input required, and its property of reducing the imperfection of the random bit sequences while still maintaining its generation rate. The structure of the quasi-shift

register comprises four shift registers, with a selected length n = 8, as depicted in Figure 3.14. The post-processor initially starts by memorizing the generated bit from the TRBG into the first shift register, and then it performs XOR operation between shift registers. These processes are repeated several times in order to increase the complexity of the bit sequence.

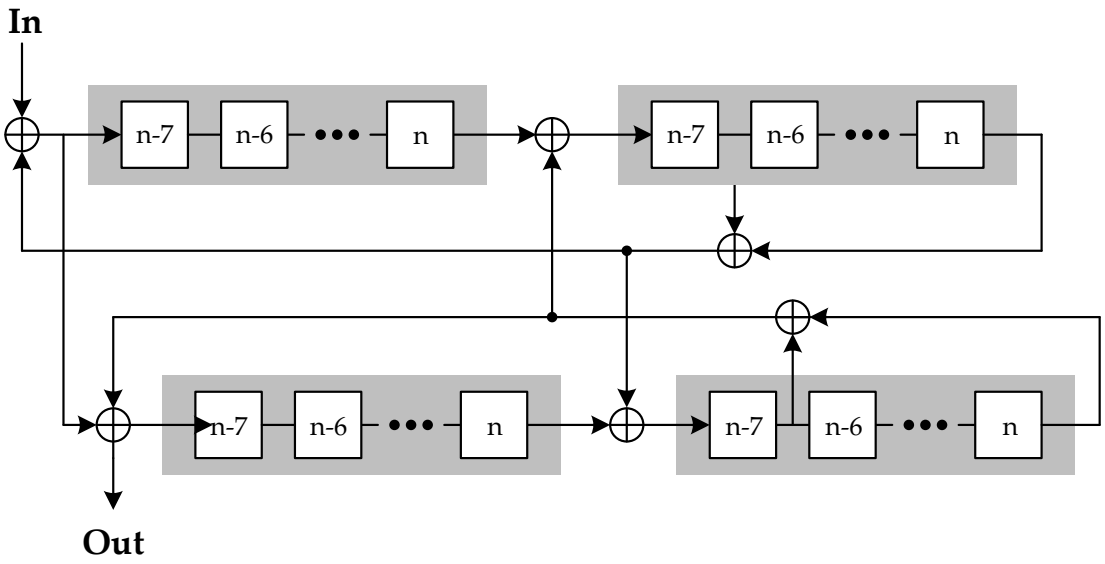

Figure 3.14. Structure of the quasi-shift register-based post-processor.

3.5 Randomness Performance Evaluation

3.5.1 NIST SP800-22 Test Suite

The random bit sequence from the TRBG was examined according to the properties of a random sequence that can be described in terms of probability. Although there are a variety of statistical tests, the NIST SP800-22 test suite is the statistical test most widely used to investigate the randomness of the output sequence from the TRBG. The NIST test suite [28], issued by the National Institute of Standards and Technology, is a statistical test package consisting of 15 tests; it is generally accepted as a standard test

suite for any random number generators. The test can be used to examine the bit sequence by detecting a pattern of values that indicates the non-randomness (periodic) of the sequences, resulting in the probability values (*P*-values). The *P*-values for each test indicate a randomness of the bit sequences, with regard to the NIST, the bit sequence that result to *P*-values greater than 0.01 is considered pass; otherwise, they are rejected. Typically, the test is considered to be passed for the proportion of the passing *P*-values that greater 0.9.

The performance of the proposed TRBG was evaluated through the NIST statistical test suite with 100 Mbit data. The generated bit sequence is divided into 100 sequences with the length of 1Mbit for each block. The proportion passing *P*-values, as shown in Table 3.3, indicate that the proposed TRBG can pass all the tests.

3.5.2 TestU01

TestU01 is a software library for statistically testing random bit generators [29]. The TestU01 library provides several test batteries, while each test battery also contains a collection of empirical statistical tests. Each statistical test can generate a *P*-value as well as the NIST test suite, which is considered as an indicator of passing the test. The test is considered passed if the generated *P*-value from the test falls into the interval [0.001, 0.999].

Three binary sequences with lengths 2^{20}, 2^{25}, and 2^{30} bits were generated from the proposed TRBG. The bit sequences were applied to the batteries Rabbit, Alphabit, and BlockAlphabit to evaluate the randomness. Each battery contains a different number of test. The Alphabit contains 17 statistical tests while the BlockAlphabit applies the Alphabit repeatedly to the reordered bits with the 6 different blocks sizes which are 1, 2, 4, 8, 16,

and 32. In other words, the BlockAlphabit contains a total number of 17 × 6 = 102 statistical tests. The Rabbit applies 38, 39, and 40 test to the bit sequence with lengths 2^{20}, 2^{25}, and 2^{30} bits, respectively. The results of the TestU01 are presented in Table 3.4. The proposed TRBG can pass all the tests.

3.5. Conclusions

In this chapter, the unified and simplified forms of the generic sigmoidal chaotic map and the linearized sigmoidal chaotic map were presented. Chaos dynamics were described in terms of chaotic waveforms, histogram, cobweb plots, fixed point, Jacobian, and a bifurcation structure diagram based on Lyapunov exponents; these revealed that both hardtanh function-based and signum function-based linearized sigmoidal chaotic maps have the potential to offer robust chaos over the entire range of parameters. In other words, it can be summarized that based on a linearized sigmoidal, the proposed sigmoidal chaotic map can offer robust chaos over the entire range of parameters. The true random bit generator based on the linearized sigmoidal chaotic map was demonstrated as a practical example; hence, the robust chaotic map is suitable as an entropy source. The resulting random bit sequence passed the NIST statistical test suite and the TestU01. Performance test results from both statistical tests show that the proposed linearized sigmoidal chaotic maps are suitable for application such as a TRBG.

Table 3.3 National Institute of Standards and Technology (NIST) statistical test suite.

Test Methods	*P*-Value	Proportion	Result
Frequency (monobit)	0.7981	0.99	Pass
Block Frequency	0.5544	0.99	Pass
Runs	0.6163	1.00	Pass
Longest Run	0.7399	1.00	Pass
Binary Matrix Rank	0.2133	1.00	Pass
Discrete Fourier Transform	0.7791	1.00	Pass
Non-overlapping Template Matching	0.4980	0.99	Pass
Overlapping Template Matching	0.9114	0.98	Pass
Universal Statistical	0.7597	0.99	Pass
Linear Complexity	0.6579	0.99	Pass
Serial	0.4983	0.98	Pass
Approximate Entropy	0.3669	1.00	Pass
Cumulative Sums	0.5139	0.99	Pass
Random Excursions	0.3322	0.98	Pass
Random Excursions Variant	0.3384	0.99	Pass

Table 3.4. TestU01

Random Bit Generator	**Test Batteries**		
	Rabbit	Alphabit	BlockAlphabit
Proposed TRBG (2^{20} bits)	38/38	17/17	102/102
Proposed TRBG (2^{25} bits)	39/39	17/17	102/102
Proposed TRBG (2^{30} bits)	40/40	17/17	102/102

Chapter 4

Parabola chaotic map with CMOS-based circuit realization

This chapter presents a new chaotic map of various parabola functions and their linearized function with regarding the proposed generic form of chaotic map with three terms which introduced in the Chapter 3. The parabola chaotic map is based on various parabola curve functions which led to the linearized parabola chaotic map using Absolute Value function. The linearized chaotic map can of offer a robust chaos over the entire range of parameter. The chaotic oscillator realizing the proposed chaotic map is designed with a simple structure and implemented using 0.18 μm CMOS technology. Simulations and analysis of the proposed chaotic map and circuit are presented to demonstrate the characteristics and chaotic behaviors. The results show that the proposed chaotic oscillator circuit offers a robust chaotic behavior for nearly the entire parameter range, which is suitable for applications where a chaotic signal is required as well as stability in generating such a signal.

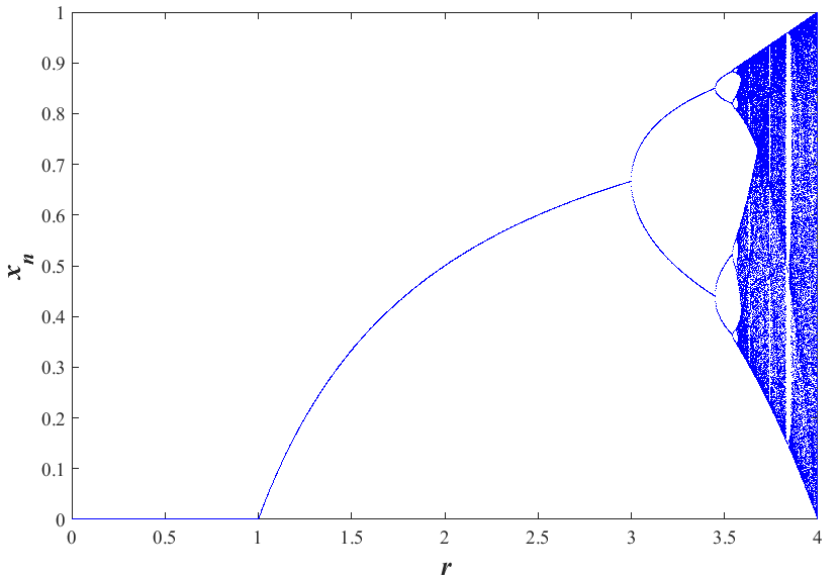

Figure 4.1 bifurcation diagrams of the Logistic map.

4.1 Introduction

Chaotic behaviors exist widely in many natural and non-natural phenomena [68]. Over the past few decades, nonlinear systems that exhibit chaotic behavior have received significant attention in various areas such as behavior modeling [69], communications [70], cryptography [71], and systems control [72]. Examples of chaotic behavior for these types of research can be provided by a discrete-time dynamic model known as a chaotic map. As chaotic oscillators are the result of realizing chaotic maps, many types of circuits and maps have been reported, including the tent map [73], the difference map [74], and the zigzag map [75].

This chapter presents a new chaotic map based on a nonlinear function with parabola transfer characteristics. Following our previous work [76], the parabola chaotic map is based on various parabola functions, including one in which the absolute value function, considered as a linearized parabola function, was employed. The chaotic

behaviors of the proposed chaotic maps were investigated using bifurcation diagrams and Lyapunov exponents. The parabola chaotic map demonstrates intermittently chaotic behavior while the linearized parabola chaotic map offers a robust chaos over the entire range of the parameter. A discrete-time chaotic oscillator circuit to create the proposed parabola chaotic map is also presented. The circuit is designed based on 0.18 µm CMOS technology. The chaotic behaviors of the circuit are described through bifurcation diagrams and chaotic waveforms. Simulation results indicate that the proposed chaotic oscillator can offer robust chaos for nearly the entire range of the parameter.

4.2 Chaotic map based on a parabola function

4.2.1 Previous Work

The Logistic map is a first-order difference equation that widely arises in the economic, social and biological sciences. The map is a one-dimensional discrete-time chaotic map and mathematically, the logistic map can be defined as

$$x_{n+1} = rx_n\left(1 - x_n\right) \tag{4.1}$$

where the parameter $r \in [0, 4]$ and variable x_n is limited into the interval [0, 1]. Equilibrium point (or fixed point) is the element of a function's domain that maps to itself. The Logistic map's equilibrium point x^* can be calculated by substituting x^* into x_n and x_{n+1} in (4.1). As a result, the equation becomes

$$x^* = rx^*\left(1 - x^*\right) \tag{4.2}$$

Solving Eq. (4.2) yields two equilibrium points which is 0 and (r – 1)/r. Figure 4.1 shows bifurcation diagram of the Logistic map with the change of its parameter r.

Observed from the bifurcation diagram, the Logistic map offers chaotic behavior when r ∈ [3.6, 4].

Standing alongside the well-known chaotic maps, such as the tent map, logistic map, and gauss map, the sigmoidal chaotic map developed in our previous work [77] was described as

$$x_{n+1} = \mp A f_{\mathrm{NL}}(B x_n) \pm C x_n \pm D \tag{4.3}$$

where the parameters A, B, C, and D are real constants, x_n is a real variable, and $f_{NL}(x)$ is any S-shaped nonlinear function or so-called sigmoidal. It can be seen from Eq. (4.3) that the sigmoidal chaotic map is different from a typical chaotic map in that it can offer different behavior based on the sigmoidal function that is used.

4.2.2 Parabola chaotic map

Motivated by the sigmoidal chaotic map, in which the nonlinear function can be replaced by any S-shaped nonlinear function, the question of whether it is possible to replace the sigmoidal function with other nonlinear functions arose. Thorough investigations led to the creation of a chaotic map using parabola functions. The proposed parabola chaotic map can be defined by a simple mathematical model of the form

$$x_{n+1} = \mp A f_{\mathrm{NL}}(B x_n) \pm C \tag{4.4}$$

where the parameters A and B are real constants, x_n is a real variable, and $f_{NL}(x)$ is a parabola function. A summary of the chaotic maps based on Eq. (4.4) using various parabola functions is shown Table 4.1 Moreover, it is apparent that the proposed chaotic map based on Eq. (4.5) is a conjugation of two chaotic maps, which can be expressed as

$$x_{n+1} = A f_{\mathrm{NL}}(B x_n) - C \tag{4.5}$$

$$x_{n+1} = -Af_{\mathrm{NL}}(Bx_n) + C \tag{4.6}$$

Table 4.1 Summary of three parabola chaotic maps involving the nonlinear functions $f_{\mathrm{NL}}(\mathrm{x})$ with parabola transfer characteristics

Case	Description	$f_{NL}(x)$ with no parameters	Chaotic maps
PM1	Polynomial function with even degree	$f_{\mathrm{NL1}}(x) = \left(x\right)^N$	$x_{n+1} = \mp A\left(Bx_n\right)^N \pm C$
PM2	Gaussian function	$f_{\mathrm{NL2}}(x) = e^{-x^2}$	$x_{n+1} = \mp Ae^{-Bx^2} \pm C$
PM3	Hyperbolic cosine function	$f_{\mathrm{NL3}}(x) = \cosh\left(x\right)$	$x_{n+1} = \mp A\cosh\left(Bx\right) \pm C$

Chaotic behavior can be investigated qualitatively and quantitatively through the use of bifurcation diagrams and Lyapunov exponents (LE). While a bifurcation diagram indicates possible long-term values of a system, involving fixed points or periodic orbits, as a function of a bifurcation parameter, the LE is widely accepted as an indicator of the existence of chaos as it represents the average divergence of two close trajectories in a dynamic system. An LE can be defined as

$$\mathrm{LE} = \lim_{\mathrm{n}\to\infty} \frac{1}{\mathrm{N}} \sum_{\mathrm{n=1}}^{\mathrm{N}} \log_2 \frac{\mathrm{dx_{n+1}}}{\mathrm{dx_n}} \tag{4.7}$$

where N is the number of iterations. A positive value of LE indicates chaotic behavior in dynamic systems, and the larger the value, the higher the degree of chaos.

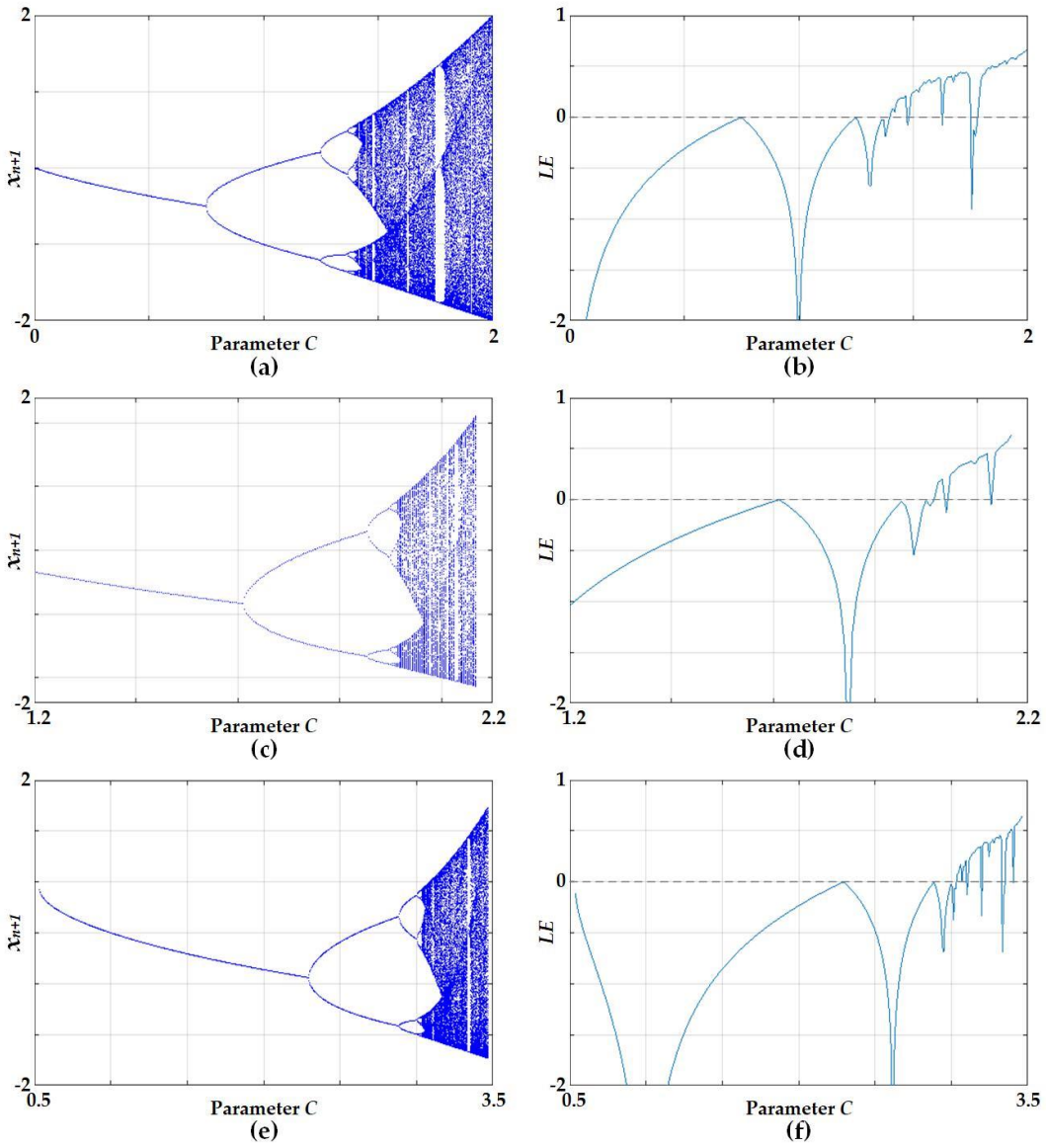

Figure 4.2 Bifurcation diagrams (left) and Lyapunov exponent (LE) plots (right) of the parabola chaotic maps with A = 1 and B = 1; (a, b) case PM1, (c, d) case PM2, and (e, f) case PM3.

In order to identify the chaotic behavior as well as the continuity of the proposed parabola chaotic maps in Eq. (4.5), both bifurcation diagrams and LE plots were employed, as shown in Figure 4.2. Parameters A and B were set to 1, while parameter C was used as the bifurcation parameter. The bifurcation diagrams in Figs. 1a, 1c, and 1e

depict a similarity of chaotic behavior of the parabola chaotic maps for cases PM1, PM2, and PM3, respectively. It is notable that the bifurcation diagrams appear to have some periodic windows and illustrate discontinuously chaotic behavior, which correspond to the LE plots. This means the parabola chaotic maps for all three cases offer robust chaos for some portion of parameter C.

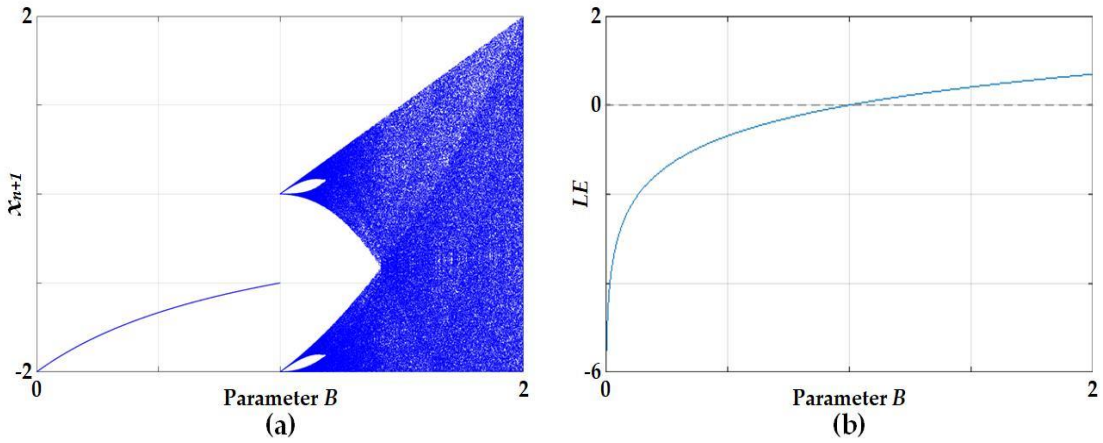

Figure 4.3 Bifurcation diagram (left) and Lyapunov exponent (LE) plot (right) of the linearized parabola chaotic map in Eq. (8) at specified parameters B = 1 and C = 1.

4.2.3 Linearization of parabola chaotic map

In addition to the use of nonlinear functions with parabola transfer characteristics, the proposed parabola chaotic map can also use a triangular function, such an absolute value function, which can be considered a linearized parabola function. Therefore, the linearized parabola chaotic map is described as

$$x_{n+1} = \mp A\left|Bx_n\right| \pm C \tag{4.8}$$

Similar to the proposed parabola chaotic map in Eq. (2), the linearized parabola chaotic map based on the absolute value function is also a conjugate of two chaotic maps,

which can also be expressed as

$$x_{n+1} = A\left|Bx_n\right| - C \tag{4.9}$$

$$x_{n+1} = -A\left|Bx_n\right| + C \tag{4.10}$$

Figure 4.3 illustrates the bifurcation diagram and LE plot of the linearized parabola chaotic map based on the absolute value in Eq. (4.10). Parameter A is the parameter used to generate the bifurcation, while parameters B and C are set to 1. As seen in the corresponding LE plot, the bifurcation diagram of the linearized parabola chaotic map shows continuously chaotic behavior over the entire range of parameter A.

The dynamic behavior of the linearized parabola chaotic map is analyzed using the Jacobian which can be found through of the first derivative as

$$J(x_n) = \frac{d(x_{n+1})}{dx} \tag{4.11}$$

Typically, the discrete time system needed to becomes unstable in order to induce the chaos which happened in the case where $|J(x_n)| > 1$. The discrete-time chaotic map can generate chaotic signals though a nonlinear iteration function (chaotic map) which can be defined as follows:

$$X_{n+1} = f\left(X_n\right) \tag{4.12}$$

The chaotic map typically has a point where x* = f(x*) which is the element of a function's domain that maps to itself and this is considered an equilibrium point (or fixed point). Table 4.2 summarizes the fixed points and Jacobians of the linearized sigmoidal chaotic maps based on the absolute value function.

Table 4.2 Summary of the fixed points of the linearized sigmoidal chaotic maps.

Chaotic Map Equations	Fixed Points x^*	Jacobian
(4.9)	$\frac{C}{1 \pm AB}$	$AB\,\mathrm{sign}(Bx)$
(4.10)	$\frac{C}{-1 \pm AB}$	$-AB\,\mathrm{sign}(Bx)$

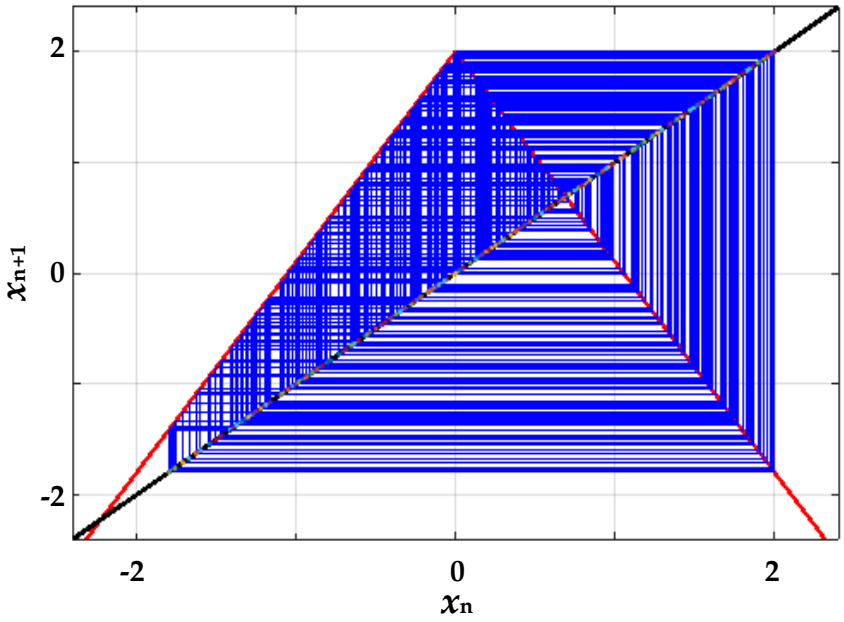

Figure 4.4 Plots of Cobweb of the linearized parabola chaotic maps based on Absolute Value on (4.11) at specific parameter A = 1.9, B = 1, and D = 1.

Other than the proposed measurement tool, a cobweb plot, which is typically a graphical method, is employed in chaotic map in order to investigate the long-term status of an initial condition under repeated application as qualitative behaviors of one-dimensional iterated function. In cobweb plot, a stable fixed point corresponds to an inward spiral while an unstable fixed point is an outward one. A chaotic orbit would show

a thick area, indicating an infinite number of nonrepeating values.

The cobweb plots of the linearized parabola chaotic maps based on Absolute Value on (4.10) at specific parameters is depicted in Figures 4.4, which were arbitrarily selected with regard to the chaotic regime, as seen in the bifurcation diagram in Figures 4.3. The boundary values of x_{n+1} observed from the cobweb plots shows that the value of x_{n+1} fall into the region (−1, 1) which also agreed to the bifurcation diagram.

4.3 Discrete-time parabola chaotic oscillator

4.3.1 Circuit designs and implementations

Eq. (2) models a parabola chaotic map consisting of three control parameters A, B, and C. For the benefit of creating a simple circuit, the chaotic map equation is rewritten in a simpler form by setting parameter B equal to 1 and considering parameter C equal to parameter A. As a result, with reference to Eq. (4.6), the parabola chaotic map with one control parameter can be described as

$$x_{n+1} = A\left(1 - f\left(x_n\right)\right) \tag{4.13}$$

Typically, a discrete-time chaotic oscillator in voltage mode requires two sample and hold circuits in order to generate a chaotic signal, as well as a nonlinear circuit. Using the parabola chaotic map equation with one control parameter in Eq. (4.13), the chaotic oscillator circuit was designed as shown in Figure 4.5. It is notable that the chaotic oscillator consists of a nonlinear circuit constructed out of three transistors, a voltage subtractor Op Amp with bias voltage V_b, and two sample and hold circuits based on a transmission gate. The size (W/L) of transistors M1, M2, and M3 are 4/0.18 µm, 0.54/0.54 µm and 4/0.18 µm, respectively. Hence, the transfer function of the nonlinear circuit in

Figure 4.5 can be written as

$$V_{out} = f_p\left(V_{in}\right) \tag{4.14}$$

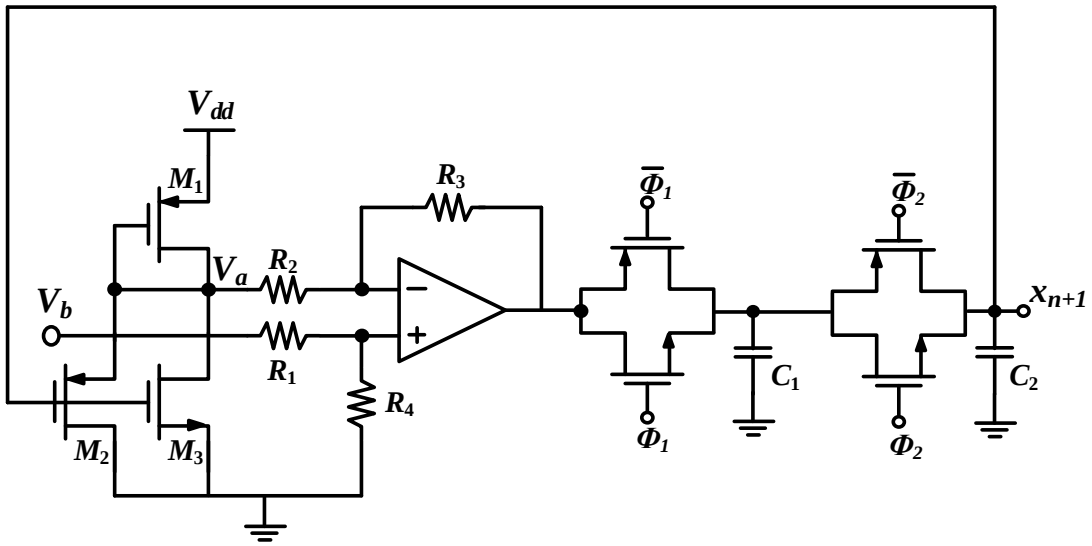

Figure 4.5 The chaotic oscillator circuit based on the parabola chaotic map model with one control parameter in Eq. (4.13).

The value of resister R_1 was set equal to R_2, and resister R_3 was set equal to R_4, so the transfer function of the subtract circuit can be defined as

$$V_{out} = \alpha(V_b - V_a) \tag{4.15}$$

where the voltage gain α is given by

$$\alpha = \frac{R_3}{R_1} \tag{4.16}$$

Consequently, the transfer function of the proposed chaotic oscillator circuit in Figure 4.4 with a specific bias voltage value of V_b=1V can be expressed as

$$x_{n+1} = \alpha\left(1 - f_p\left(x_n\right)\right) \tag{4.17}$$

It can be seen that the transfer function of the proposed chaotic oscillator

corresponds to the parabola chaotic map equation with one control parameter in Eq. (4.13).

4.3.2 Simulation results

The proposed CMOS chaotic oscillator circuit has been implemented based on 0.18 μm CMOS technology using a Cadence virtuoso environment. The chaotic oscillator circuit is supplied with 1.8 V driven by two non-overlapping clocks (Φ_1 and Φ_2) of 500 kHz. In HSPICE simulation.

To confirm the validity of the chaotic oscillator, the output signals, resulting from varying the voltage gain α in the range of 0–2, were used to plot the bifurcation diagram shown in Figure 4.6a. The output waveform in transient of the chaotic oscillator where the voltage gain α was set to 1.9 resulted in an output voltage between 0.78 V and 1.17 V, as shown in Figure 4.6b. It can be clearly seen from the bifurcation diagram that only one periodic window exists. In other words, a proposed chaotic oscillator circuit based on the parabola chaotic map can offer a robust chaotic behavior for nearly the entire range of voltage gain.

4.4 Conclusion

In this chapter, a chaotic map based on parabola functions and their linearized function has been presented. The chaotic behaviors were investigated through bifurcation diagrams and LE plots. The linearized parabola chaotic map based on a nonlinear such an Absolute Value function has revealed that the parabola chaotic maps also have the potential to offer robust chaos over the entire range of parameters. The operation of the chaotic oscillator circuit realizing the proposed map was verified by HSPICE simulations.

The results show that the circuit can provide a similar chaotic behavior to the proposed chaotic map can offer robust chaos nearly the entire range of parameter

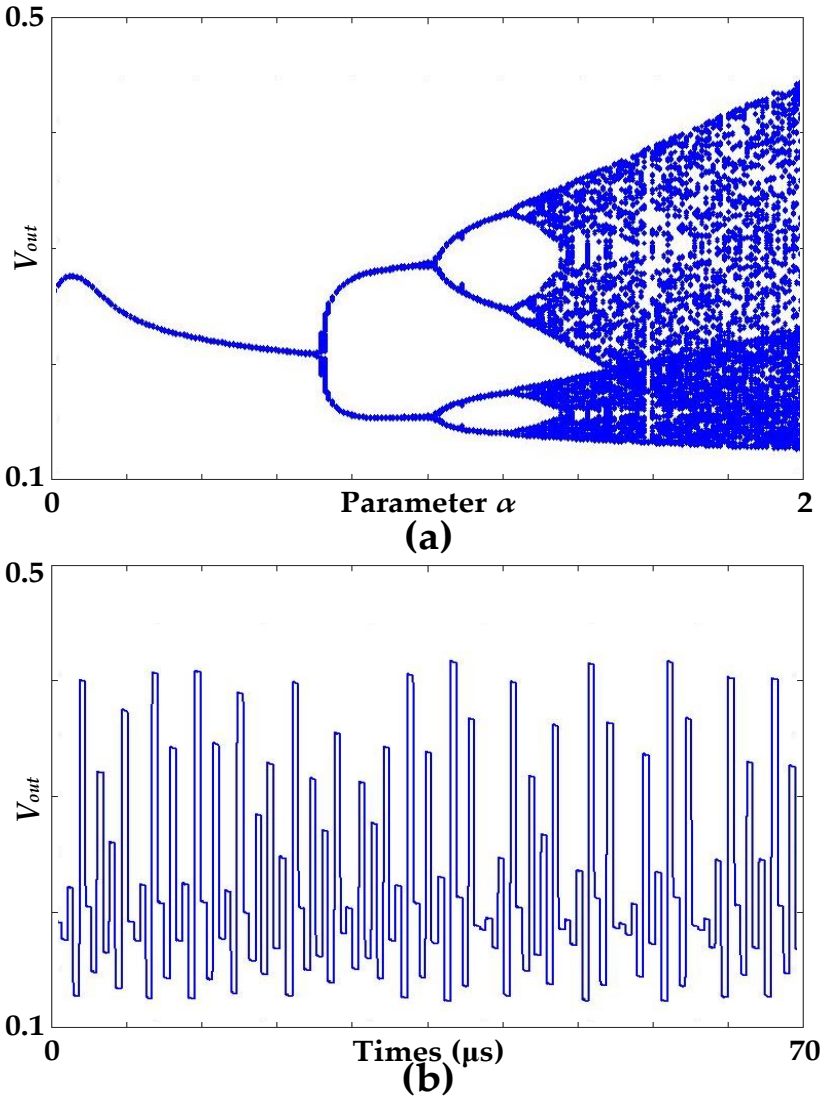

Figure 4.6 Bifurcation diagram and Lyapunov exponent (LE) plot of the proposed chaotic oscillator.

Chapter 5

Conclusion and Discussions

This dissertation has presented new chaotic oscillator circuits as well as new chaotic maps. Additionally, the development of true random bit generators based on the proposed chaotic oscillators are also demonstrated. Chapter 1 has introduced the chaos theory, many measurement tools for chaotic dynamics and random number generator. The main objective of this dissertation is to develop new chaotic oscillators as well as research and investigation on new chaotic maps and their chaotic dynamic. The designed chaotic oscillators are expected to be simple, compact, and offer robust chaotic behavior. Other than chaotic oscillator, new chaotic maps are also presented. The chaotic dynamics of each proposed chaotic oscillators and the proposed chaotic maps are investigated through various methods such as the quantitative and qualitative tools which are the plot of bifurcation diagram and LEs, respectively, or the system stability analysis using Jacobian and fixed point. Moreover, the true random bit generators, which considered major part of cryptography, designed based on various proposed chaotic oscillator are demonstrated as a practical example of chaos-based application and the output is statistically tested in order to shows the feasibility of the proposed chaotic oscillator circuits as a randomness source for the generator.

The design strategy for the chaotic oscillators are based on the hypothesis, which

can be defined that the chaotic oscillator circuit can be built by using a nonlinear circuit with the specific transfer characteristic such as approximate V-shape or N-shape, and also based on the circuit realization of the new chaotic map so call sigmoidal chaotic map and parabola chaotic map.

As for the proof of the hypothesis as mentioned above, the chapter 2 has presented two discrete time chaotic oscillators. The first chaotic oscillator is a compact circuit based on chaotic map with only 3 transistors in order to achieve an approximate V-shape characteristic. The second proposed chaotic oscillator is based a chaotic map which is constructed in order achieve a reverse sigmoid characteristic. This chaotic oscillator exhibits a robust chaotic behavior which can be seen from the plot of bifurcation diagram. Other than the proposed of the research and study on chaotic oscillators, this chapter proposed a true random number generator (TRBG) based on discrete-time chaotic oscillator which can offer a throughput of 23 Mbps and the output bit sequence is evaluated NIST tests suite which can pass all the test. Subsequently, a hybrid random number generator (HRBG) based on a combination of TRBG and pseudo random bit generator (PRBG). The output of chaotic oscillator based TRNG and linear feedback shift register (LFSR) are XORed together to produce a random bit output. By such a simple structure, the proposed HRNG provides a throughput of 1 Mbps which has been statistically analyzed through NIST statistical tests suite and proved to be suitable for cryptography.

In chapter 3, the unified and simplified forms of the generic sigmoidal chaotic map and the linearized sigmoidal chaotic map were presented. Chaos dynamics were described in terms of chaotic waveforms, histogram, cobweb plots, fixed point, Jacobian, and a bifurcation structure diagram based on Lyapunov exponents; these revealed that

both hardtanh function-based and signum function-based linearized sigmoidal chaotic maps have the potential to offer robust chaos over the entire range of parameters. In other words, it can be summarized that based on a linearized sigmoidal, the proposed sigmoidal chaotic map can offer robust chaos over the entire range of parameters. The true random bit generator based on the linearized sigmoidal chaotic map was demonstrated as a practical example; hence, the robust chaotic map is suitable as an entropy source. The resulting random bit sequence passed the NIST statistical test suite and the TestU01. Performance test results from both statistical tests show that the proposed linearized sigmoidal chaotic maps are suitable for application such as a TRBG.

Finally, chapter 4 has presented the parabola chaotic map with simplified and linearized forms based on the generic form of chaotic map proposed in the Chapter 3. Chaos dynamics were described in terms of fixed point, Jacobian, chaotic waveforms, cobweb plots, bifurcation diagram, and Lyapunov exponents. As a result, the linearized parabola chaotic map based on a nonlinear such an Absolute Value function has revealed that the parabola chaotic maps also have the potential to offer robust chaos over the entire range of parameters. In other words, it may be able to assumed that the linearized chaotic map based on the proposed generic form of chaotic map offer robust chaos over the entire range of parameters. A new chaotic oscillator based on parabola chaotic map was introduced. The proposed chaotic oscillator was designed based on 0.18 μm CMOS technology through the use of 3 transistors with subtractor Op Amp to construct a compact chaotic map circuit. Simulation results of the circuit indicate the proposed chaotic oscillator can offer robust chaos nearly the entire range of parameter

This dissertation has proposed many chaotic oscillator implementations using a simple structure. Simulation results show the feasibility and compatibility for application

based on all the proposed chaotic oscillators. The true random bit generators based on each proposed chaotic oscillator were presented with the statistical evaluation. It can be concluded that chaotic oscillator circuit can be achieved by using a nonlinear circuit with specific transfer characteristic such as V-shape or S-shape (sigmoid) characteristic Moreover, a research and study on two new chaotic maps are also presented. The proposed chaotic maps were developed, with regarding to conclusion of the proposed chaotic oscillators, based on sigmoidal function and parabolic function. Furthermore, the proposed chaotic maps based on the linearized functions have demonstrated the robustness property of chaotic system.

References

[1] S. Strogatz, Nonlinear Dynamics and Chaos, 2nd ed., CRC Press, 2018

[2] T. Shu, Uniform random numbers: Theory and practice, Kluwer Academic Publishers, 1995.

[3] Schneier B. Applied cryptography. 2nd ed., New York: Wiley;1996

[4] Manuel Delgado-Restituto, Rafael Lopez de Ahumada, and Angel Rodriguez-Vgzque, “Secure Communication though Switched-Current Chaotic Circuits,” IEEE Trans. On Circuits and Systems, vol. 3, pp. 2237-2240, 1995.

[5] Stefano Gregori, Alessandro Cabrini, “CMOS Discrete-Time Chaotic Circuit for Low-Power Embedded Cryptosystems,” IEEE Trans. On Circuits and Systems, vol. 2, pp. 1498-1501, August 2005.

[6] C.S. Petrie and J.A. Connelly, "A Noise-Based IC Random Number Generator for Applications in Cryptography," IEEE Trans. Circuits and Systems I, vol. 47, no. 5, pp. 615-621, May 2000.

[7] Kolumbán, Géza, Michael Peter Kennedy, and Leon O. Chua. "The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications." IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 44, no. 10, 1997.

[8] P. Ping, F. Xu, and Z. J. Wang, “Image encryption based on nonaffine and balanced cellular automata,” Signal Process., vol. 105, no. 12, pp. 419–429, 2014.

[9] G. Millerioux, J. M. Amigo, and J. Daafouz, “A connection between chaotic and conventional cryptography,” IEEE Transactions on Circuits and Systems I, Regular Papers, vol. 55, no. 6, pp. 1695–1703, Jul. 2008.

[10] K. Cho and T. Miyano, “Chaotic cryptography using augmented Lorenz equations aided by quantum key distribution,” IEEE Transactions on Circuits and Systems I, Regular Papers, vol. 62, no. 2, pp. 478–487, Feb. 2015.

[11] Angel Rodriguez-Vizquez, and Manuel Delgado-Restituto, “CMOS Design of Chaotic Oscillators Using State Variables: A Monolithic Chua’s Circuitt,” IEEE Transactions on Circuits and Systems I: Analog and Digital Signal Processing, vol. 40, no. 10, 1993.

[12] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, and J. M. Bahi, “Theoretical design and FPGA-based implementation of higher dimensional digital chaotic systems,” IEEE Transactions on Circuits and Systems I, Reg. Papers, vol. 63, no. 3, pp. 401–412, Mar. 2016.

[13] X. Wang and Z. Cheng, “Synchronization of coupled discrete-time harmonic oscillators with rational frequency,” IEEE Transactions on Automatic Control, vol. 58, no. 6, pp. 1573–1579, 2013.

[14] C. Shen, S. Yu, J. Lu, and G. Chen, “Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model,” IEEE Transactions on Circuits and Systems I, Regular Papers, vol. 61, no. 8, pp. 2380–2389, Aug. 2014.

[15] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, “Cascade chaotic system with applications,” IEEE Transactions on Cybernetics, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[16] Y. Wu, Y. Zhou, and L. Bao, “Discrete wheel-switching chaotic system and applications,” IEEE Transactions on Circuits and Systems I, Regular. Papers, vol. 61, no. 12, pp. 3469–3477, Dec. 2014.

[17] Y. Zhou, L. Bao, and C. L. P. Chen, “A new 1D chaotic system for image encryption,” Signal Process., vol. 97, pp. 172–182, Apr. 2014.

[18] Liu, Hai-Feng, et al. "The largest Lyapunov exponent of chaotic dynamical system in scale space and its application." Chaos: An Interdisciplinary Journal of Nonlinear Science vol. 13, no. 3, 2003.

[19] Testa, James, José Pérez, and Carson Jeffries, "Evidence for universal chaotic behavior of a driven nonlinear oscillator," Physical Review Letters, vol. 48, no. 11, 1982.

[20] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, “Determining Lyapunov exponents from a time series,” Phys. D, Nonlinear Phenomena, vol. 16, no. 3, pp. 285–317, 1985.

[21] May, Robert M. "Simple mathematical models with very complicated dynamics," Nature, vol. 261, no. 5560, 1976.

[22] Arrowsmith, David, and Colin M. Place. Dynamical systems: differential equations, maps, and chaotic behaviour. Vol. 5. CRC Press, 1992.

[23] Salih Ergüna, Serdar Özo˜guz, “Truly random number generators based on a non-autonomous chaotic oscillator,” AEU - International Journal of Electronics and Communications, vol. 61, pp. 225-242, April 2007.

[24] Sergio Callegari, “Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos,” IEEE Trans. On Signal Processing, vol. 53, no. 2, February 2005.

[25] Yalcin, Mustak E., Johan AK Suykens, and Joos Vandewalle, "True random bit generation from a double-scroll attractor," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 51, no.7, 2004.

[26] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti, “A Fast Chaos-based True Random Number Generator for Cryptographic Applications,” IEEE Trans. On Solid-State Circuits, pp. 130-133, 2006.

[27] Uchida, Atsushi, et al, "Fast physical random bit generation with chaotic semiconductor lasers," Nature Photonics vol. 2, no.12, 2008.

[28] A. Rukin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” National Institute of Standards and Technology: Gaithersburg, MD, USA, 2001.

[29] P. L'Ecuyer, and R. Simard, “TestU01: AC library for empirical testing of random number generators,” ACM Trans. on Mathematical Software, vol. 33, no. 4, 2007.

[30] Angel Rodriguez-Vazquez, Jose L. Huertas, Adoracion Rueda, Belen Perez-Verdu, and Leon O. Chua, “Chaos from Switched-Capacitor Circuits: Discrete Map”, Proceedings of the IEEE, vol. 75, pp. 1090-1161, 1987.

[31] Eckmann, J-P., and David Ruelle, "Ergodic theory of chaos and strange attractors." The Theory of Chaotic Attractors. Springer, New York, NY, 1985.

[32] Lorenz, Edward N., and K. Haman. "The essence of chaos." Pure and Applied Geophysics, vol. 147, no. 3, 1996.

[33] Tabor, Michael. Chaos and integrability in nonlinear dynamics: an introduction. Wiley, 1989.

[34] Dudek, P., and V. D. Juncu, "Compact discrete-time chaos generator circuit," Electronics Letters vol. 39, no. 20, 2003.

[35] V.D. Juncu, M. RafieI-naeini, and P. Dudek, “Integrated Circuit Implementation of a Compact Discrete-Time Chaos Generator,” Analog Integrated Circuits and Signal Processing, vol. 46, pp. 275–280, 2006.

[36] Valtierra, José Luis, Esteban Tlelo-Cuautle, and Ángel Rodríguez-Vázquez. "A switched-capacitor skew-tent map implementation for random number generation." International Journal of Circuit Theory and Applications, vol. 45, no. 2, 2017.

[37] Nejati, Hamid, Ahmad Beirami, and Yehia Massoud, "A realizable modified tent map for true random number generation." IEEE 51st Midwest Symposium on Circuits and Systems (MWSCAS), 2008.

[38] Katz, Oded, Dan A. Ramon, and Israel A. Wagner. "A robust random number generator based on a differential current-mode chaos." IEEE Transactions on very large scale integration (VLSI) systems vol. 12, 2008.

[39] Johansson, Anders J., and Henrik Floberg, "Random number generation by chaotic double scroll oscillator on chip," Proceedings of the 1999 IEEE International Symposium on Circuits and Systems (ISCAS), vol. 5, pp. 407-409. 1999.

[40] Avaroğlu, Erdinç, et al, "Hybrid pseudo-random number generator for cryptographic systems," Nonlinear Dynamics vol. 82, 2015.

[41] Avaroglu, Erdinç, et al, "A new method for hybrid pseudo random number generator," Informacije MIDEM vol. 44, 2015.

[42] M. Majumdar, and T. Mitra, “Robust Ergodic Chaos in Discounted Dynamic Optimization Models,”. Econ. Theory, no. 4, pp. 677–688, 1994.

[43] R. Dogaru, A. T. Murgan, S. Ortmann, and M. Glesner, “Searching for Robust Chaos in Discrete Time Neural Networks using Weight Space Exploration,” Int. Conf. Neural Network, no. 2, pp. 688–693, 1996.

[44] S. Banerjee, J. A. Yorke, and C. Grebogi, “Robust Chaos,” Phys. Review Letter, no. 80, pp. 3049–3052, 1998

[45] P. K. Shukla, A. Khare, M. A. Rizvi, S. Stalin, and S. Kumar, “Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing,” Entropy, vol. 17, pp. 1387–1410, 2015.

[46] X. Wang, Y. Zhang, and X. Bao, “A Colour Image Encryption Scheme Using Permutation-Substitution Based on Chaos,” Entropy, vol. 17, pp. 3877–3897, 2015.

[47] K. Fallahi, and H. Leung, “A Chaos Secure Communication Scheme Based on Multiplication Modulation,” Communication. Nonlinear Science Numerical Simulation, vol. 15, pp. 368–383, 2010.

[48] A. N. Miliou, I. P. Antoniades, S. G. Stavrinides, and A. N. Anagnostopoulos,” Secure Communication by Chaotic Synchronization: Robustness Under Noisy Conditions,” Nonlinear Analysis: Real World Applications, vol. 8, pp. 1003–1012, 2007.

[49] G. Xu, Y. Shekofteh, A. Akgül, C. Li, and S. Panahi, “A New Chaotic System with a Self-Excited Attractor: Entropy Measurement, Signal Encryption, and Parameter Estimation,” Entropy, vol. 20, no. 86, 2018.

[50] W. San-Um, and W. Srichavengsup, “A Robust Hash Function Using Cross-Coupled Chaotic Maps with Absolute-Valued Sinusoidal Nonlinearity,” International Journal of Advanced Computer Science and Applications, vol. 7, no.1, 2016.

[51] M. Andrecut, and M. Ali, “On The Occurrence of Robust Chaos in a Smooth System,” Modern Physics Letters, vol. 15, pp. 391–395, 2001.

[52] M. Andrecut, and M. Ali, “Robust Chaos in a Smooth System,” International Journal of Modern Physics, vol. 15, no. 02, 2001.

[53] G. Pérez, “Robust Chaos in Polynomial Unimodal Maps,” International Journal of Bifurcation and Chaos, vol. 14, pp. 2431–2437, 2004.

[54] O. Alvarez-Llamoza, M. G. Cosenza, and G. A. Ponce, “Critical Behavior of the Lyapunov Exponent in Type-III Intermittency,” Chaos Solitons Fractals, vol. 36, pp. 150–156, 2008.

[55] J. M. Aguirregabiria, “Robust Chaos with Prescribed Natural Invariant Measure and Lyapunov Exponent,” arXiv:0907.3790, 2009.

[56] J. Hrusak, D. Mayer, and M. Stork, “Structural Synthesis of State Space Energy Based Adaptive Controller for Robust Chaos-Generating Systems of Arbitrary Finite Order,” Proceedings of the International Conference on Applied Electronics (AE), pp. 107–110, 2012.

[57] E. V. Nikulchev, “Robust Chaos Generation On the Basis of Symmetry Violations in Attractors,” Proceedings of the 2nd International Conference on Emission Electronics (ICEE), pp. 1-3, 2014.

[58] E. V. Nikulchev, “Generation of Robust Chaos in The Invariant Centre Manifold,” Proceedings of the International Conference "Stability and Control Processes" in Memory of V.I. Zubov (SCP), pp. 290-291, 2015.

[59] Z. Elhadj, and J. C. Sprott, “Is A Unifying Chaotic Dynamical System Possible?,” International Journal of Open Problems in Computer Science and Mathematics, vol. 5, pp. 75-78, 2012.

[60] Z. Elhadj, and J. C. Sprott, “The Unified Chaotic System Describing the Lorenz and Chua Systems,” Facta Universitatis, vol. 23, pp. 345-355, 2010.

[61] Z. Elhadj, and J. C. Sprott , “Unified Piecewise Smooth Chaotic Mapping that Contains the Hénon and the Lozi Systems,” Annual Review of Chaos Theory, Bifurcations and Dynamical Systems, vol. 1, pp. 50-60, 2011.

[62] N. Marwan, M. C. Romano, M. Thiel, and J. Kurths, “Recurrence Plots for The Analysis of Complex Systems,” Physics Reports, vol. 438, pp. 237-329, 2007.

[63] H. Nejati, A. Beirami, and W. H. Ali, “Discrete-Time Chaotic-Map Truly Random Number Generators: Design, Implementation, and Variability Analysis of the Zigzag Map,” Analog Integrated Circuits Signal Process, vol. 73, pp. 363-374, 2012.

[64] S. Callegari, R. Rovatti, and G. Setti, “Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos,” IEEE Trans. Signal Processing, vol. 53, pp. 793-805, 2005.

[65] L. Liu, S. Miao, H. Hu, and Y. Deng, “Pseudorandom Bit Generator Based on Non-Stationary Logistic Maps,” IET Information Security, vol. 10, pp. 87-94, 2016.

[66] Z. Elhadj, and J. C. Sprott, “On The Robustness of Chaos in Dynamical Systems: Theories and Applications,” Frontiers of Physics in China, vol. 3, pp. 195-204, 2008.

[67] F. Pareschi, R. Rovatti, and G. Setti, “Simple and Effective Post-Processing Stage for Random Stream Generated by A Chaos-Based RNG,” Proceedings of NOLTA, 2006.

[68] C. Letellier: *Chaos in nature* (World Scientific, Singapore, 2013).

[69] M. Rosalie, *et al*.: "Chaos-enhanced mobility models for multilevel swarms of UAVs," Swarm and Evolutionary Computation vol. 41, 2018.

[70] G. Kaddoum: "Wireless chaos-based communication systems: A comprehensive survey," IEEE Access vol. 4, 2016.

[71] E. Yavuz, *et al*.: “A chaos-based image encryption algorithm with simple logical functions,” Computers & Electrical Engineering vol. 54, 2016.

[72] T.B.T Nguyen, *et al*.: "Adaptive sliding mode control of chaos in permanent magnet synchronous motor via fuzzy neural networks," Mathematical Problems in Engineering, 2014.

[73] I. Campos-Cantón, *et al*.: "A simple electronic circuit realization of the tent map," Chaos, Solitons and Fractals vol. 42, 2009.

[74] M. García-Martínez, *et al*.: "Difference map and its electronic circuit realization," Nonlinear Dynamics vol. 74**,** 2013.

[75] Beirami, A., H. Nejati, and W. H. Ali. "Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator." Electronics Letters, vol. 48, no. 24, 2012.

[76] N. Jiteurtragool, *et al.*: "Robustification of a One-Dimensional Generic Sigmoidal Chaotic Map with Application of True Random Bit Generation," Entropy vol. 20, 2018.

[77] C. Shen, et al.: "Design and Circuit Implementation of Discrete-Time Chaotic Systems with Modulus of Triangular Wave Functions," International Journal of Bifurcation and Chaos vol. 24**,** 2014.

[78] Jiteurtragool, N., et al. "Low-power discrete-time CMOS chaotic oscillator based on approximated non-linear characteristic." TENCON 2014-2014 IEEE Region 10 Conference. IEEE, 2014.

[79] Fabio Pareschi, Gianluca Setti, and Riccardo Rovatti. Implementation and testing of high-sp eed cmos true random numb er generators based on chaotic systems. IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 12, 2010.

[80] H.L.D.S. Cavalcante, D.J. Gauthier, J.E.S. Socolar, and R. Zhang. On the origin of chaos in autonomous boolean networks. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 368, 2010.

[81] Johannes Norrell, Bjorn Samuelsson, and Joshua E. S. Socolar. Attractors in continuous and boolean networks. Physical Review E, vol. 76, 2007.

[82] B. Jun and P. Kocher, "The Intel Random Number Generator," Cryptography Research Inc., white paper prepared for Inter Corp., 1999,

[83] Schneier B. Applied cryptography. 2nd ed., New York: Wiley;1996

[84] Fairfield, R. C., R. L. Mortenson, and K. B. Coulthart. "An LSI random number generator (RNG)." Advances in cryptology. Springer Berlin Heidelberg, 1985.

[85] Kwok, Siew-Hwee, et al. "A comparison of post-processing techniques for biased random number generators." Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication. Springer Berlin Heidelberg, 2011.

[86] Park, Myunghwan, John C. Rodgers, and Daniel P. Lathrop. "True random number generation using CMOS Boolean chaotic oscillator." Microelectronics Journal, vol. 46, no. 12, 2015.

[87] P. Ashwin, “Nonlinear dynamics: Synchronization from chaos,” Nature, vol. 422, no. 6930, pp. 384–385, 2003.

Lists of Publications

Journals

1. Nattagit Jiteurtragool, Tachibana Masayoshi, and Wimol San-Um, “Robustification of a One-Dimensional Generic Sigmoidal Chaotic Map with Application of True Random Bit Generation”, Entropy, Vol. 20, No. 2, 2018.

2. Nattagit Jiteurtragool, Tachibana Masayoshi, Chatchai Wannaboon and Wimol San-Um, “Parabola chaotic map with CMOS-based circuit realization”, IEICE Electronics Express (Submitted).

Conferences

1. Nattagit Jiteurtragool, Tachibana Masayoshi “True Random Number Generator Based on Compact Chaotic Oscillator.” 15th International Symposium on Communications and Information Technologies, 2015.

2. Nattagit Jiteurtragool, Tachibana Masayoshi “Hybrid random number generator based on chaotic oscillator.” International Conference on Management and Innovation Technology, 2016.

Acknowledgements

The author would like to express his gratitude to his family from their endless love, encouragements and supports. The author is most grateful to his advisor, Prof. Dr. TACHIBANA Masayoshi for the great opportunity to study and conduct a research under his valuable supervision and support throughout the past two year and deeply grateful to Asst. Prof. Dr. Wimol San-Um for his valuable supports and suggestions.

The author wishes to acknowledgements Kochi-University of Technology (KUT) for their financial supports. The author also wishes to thank all members of International Relation Center for their kindly support and instructions.

Finally, the author appreciates all of his Thai friends in KUT and his colleagues in LSI laboratory for their friendship and technical assistant.