UNIVERSITI PUTRA MALAYSIA

GENERATION AND STATISTICAL ANALYSIS OF CHAOS-BASED PSEUDORANDOM SEQUENCES

ALLIYU DANLADI HINA

IPM 2019 21

GENERATION AND STATISTICAL ANALYSIS OF CHAOS-BASED PSEUDORANDOM SEQUENCES

By

ALIYU DANLADI HINA

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

July 2019

COPYRIGHT

DEDICATIONS

This thesis is dedicated to all men and women of good intentions.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

GENERATION AND STATISTICAL ANALYSIS OF CHAOS-BASED PSEUDORANDOM SEQUENCES

By

ALIYU DANLADI HINA

July 2019

Chairman : **Assoc. Prof. Mohamad Rushdan MD Said, PhD**
Faculty : **Institute for Mathematical Research**

True random numbers have gained wide applications in many areas like: computer simulation, Monte Carlo integration, cryptography, randomized computation, radar ranging, and other areas. The generation of random numbers is impractical in real life because of difficulty in reproduction, even under the most legitimate requirements. Unfortunately, the output of physical random sources cannot be reproduced, and therefore cannot be used directly for cryptographic purposes. A deterministically generated pseudorandom (appear to be random) numbers are therefore relied upon. Two constructions for generating pseudorandom sequences were considered, viz: Linear feedback shift registers (LFSR) and chaos theory (discrete chaotic maps). A class of one dimensional (1D) chaotic maps has been considered for the generation of binary sequences. From within the class of these 1D maps, we dwell on those that satisfies the equidistributivity property (EDP) and constant summation property (CSP). Statistical analysis shows that there exist reasonable cross(auto)correlations within the generated sequences. These correlations are catastrophic in cryptography. Despite these short comings, the process of sequence generation using chaos theory is indeed rich in nonlinearity, which is a fundamental requirement for cryptography. A newly proposed nonlinear controlled chaotic generator (NCCG) is designed based on the combination of a chaotic map and a LFSR is presented. The generator exhibits all the good qualities of a nonlinear combiner generator which addresses one of the major shortcoming of chaos based sequences- *short period*. Due to the influence the nonlinear combiner generator may have on the generated sequences, it was tested against fast correlation attack, one of the major attacks known to weaken nonlinear combiner based sequences. The sequence is passed through the National Institute of Standards and Technology (NIST) test suites, which looked for characteristics of a truly random sequence. The generated sequences were found to have passed all the prescribed tests in the suite (exhibits behavior that is expected from a truly random sequence.), thereby, suggesting its ability to be implemented in a cryptographic algorithm. The proposed generator has been analyzed in two phases with the first phase subjected to correlation (fast) attack and the second phase by convolutional encoder based correlation attack. It was reported that the initial state of the LFSRs in the

combiner generator cannot be recovered through this attacks within available resources. Thus, we conclude that from the results of the statistical analysis, the number of observed keystream symbols cannot be recovered. This recovery is necessary for a successful attack, aimed at determining the initial state of the LFSR. If one is not able to predict the sequence generated by the combiner generator, then the clocking nature of the two chaos based binary generators cannot be understood. Therefore the final binary sequence realized from the generator (NCCG) will be appreciably resistant to the cryptanalytic algorithms considered.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

PENJANAAN DAN ANALISIS BERSTATISTIK JUJUKAN PSEUDORAWAK BERASASKAN-KEKACAUAN

Oleh

ALIYU DANLADI HINA

Julai 2019

Pengerusi : **Prof. Madya Mohamad Rushdam MD Said, PhD**
Fakulti : **Institut Penyelidikan Matematik**

Nombor rawak sebenar telah memperolehi pelbagai aplikasi dalam banyak bidang seperti: simulasi komputer, pengamiran Monte Carlo, kriptografi, pengiraan rawak, radar berjulat dan lain-lain. Penjanaan nombor rawak tidak praktikal dalam kehidupan sebenar kerana kesukaran dalam penghasilan semula, walaupun di bawah keperluan yang paling sah. Malangnya, output sumber rawak fizikal tidak dapat dihasilkan semula, dan oleh itu tidak boleh digunakan secara langsung untuk tujuan kriptografi. Oleh itu, kita bergantung kepada nombor pseudorawak yang dihasilkan secara berketentuan (yang nampak rawak). Dua pembinaan untuk menjana jujukan pseudorawak telah dipertimbangkan, iaitu: daftar peralihan maklum balas linear (LFSR) dan teori kekacauan (peta kekacauan diskrit). Satu peta kekacauan satu dimensi (1D) telah dipertimbangkan untuk penjanaan jujukan perduaan. Dari dalam kelas peta 1D ini, kita melihat kepada yang memenuhi sifat pengagihan sama (EDP) dan sifat penghasiltambahan malar (CSP). Analisis berstatistik menunjukkan terdapat hubungan korelasi (auto) silang yang munasabah dalam jujukan yang dihasilkan. Korelasi ini adalah berbahaya dalam kriptografi. Walaupun wujud kekurangan ini, proses penjanaan jujukan menggunakan teori kekacauan memang kaya dengan sifat tak linear, yang merupakan keperluan asas bagi kriptografi. Penjana kekacauan terkawal tidak linear (NCCG) baru yang dicadangkan direka berdasarkan gabungan peta kekacauan dan LFSR. Penjana ini mempamerkan semua kualiti yang baik daripada penjana gabungan tak linear yang menangani salah satu kekurangan utama jujukan berdasarkan kekacauan, iaitu kalaan yang pendek. Disebabkan pengaruh penjana gabungan tak linear pada jujukan yang dihasilkan, ia telah diuji terhadap serangan korelasi cepat, salah satu serangan utama yang diketahui untuk melemahkan jujukan berdasarkan gabungan tak linear. Jujukan seterusnya diuji melalui set ujian National Institute of Standards and Technology (NIST), dengan pencarian ciri-ciri jujukan yang benar-benar rawak. Jujukan yang dijana dilihat telah melepasi semua ujian yang ditetapkan dalam set tersebut (mempamerkan tingkah laku yang dijangka dari jujukan yang benar-benar rawak), dengan itu, mengemukakan keupayaannya untuk dilaksanakan dalam algoritma kriptografi. Penjana yang dicadangkan telah dianalisis dalam dua fasa dengan fasa pertama tertakluk kepada serangan

korelasi (cepat) dan fasa kedua serangan korelasi berasaskan pengekod konvolusi. Adalah dilaporkan bahawa keadaan awal LFSR dalam penjana gabungan tidak dapat diperolehi kembali melalui serangan ini dalam sumber yang tersedia. Oleh itu, kita menyimpulkan bahawa dari hasil analisis secara teori, bilangan simbol aliran kekunci yang diperhatikan tidak dapat dikembalikan semula. Ini adalah yang diperlukan untuk serangan yang berjaya, bertujuan untuk menentukan keadaan awal LFSR. Jika seseorang tidak dapat meramalkan jujukan yang dijana oleh penjana gabungan, maka sifat pencatatan masa dua penjana perduaan berasaskan kekacauan tidak dapat difahami. Oleh itu jujukan perduaan yang direalisasikan dari penjana (NCCG) akan kebal terhadap algoritma penyahsulitan yang dipertimbangkan.

ACKNOWLEDGEMENTS

Alhamdulillah!!!
I wish to thank my parents for seeing me through to this age, this task wouldn't have been a success without you being there for me at all times. I wish to sincerely appreciate my wife for her understanding even when she has reasons to be disturbed, my children Al'ameen, Fatima and Abubakar for enduring to be without their father for this long. My teachers at primary and secondary levels, my lecturers all through my education at tertiary levels, THANK YOU ALL. I humbly wish to appreciate my supervisors: Assoc. Prof. Dr. Rushdan MD Said for his guidance and fatherly advice, Dr Santo Banerjee and Assoc. Prof. Dr. Muhammad Rezal Kamel Ariffin for their guidance, tutoring and mentoring. My appreciation to the entire management of Federal Polytechnic Bauchi-Nigeria. The immediate Past and the current rectors Dr. Shuaibu Musa and Arch. Sanusi Muhammed Gumau respectively, the registrar Hajiya Rakiya Maleka, for the opportunity given to me to undertake this study. Their support and understanding is well appreciated. My immediate past Head of department Mal. Salihu Chimo for the confidence and opportunities given to me. The current head of department Mal Umar Pan for his continuous support, understanding and fatherly guidance. To my colleagues too numerous to mention, i say THANK YOU ALL. I want to particularly appreciate Mal. Yusuf Ilelah for being there for me at instances too numerous to mention. To my brother Mohammed Kabiru and my sister Nafisat, i appreciate your unending prayers. To all my friends, far and near, i say THANK YOU ALL.
Masha Allah!!!

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Mohamad Rushdan Md Said, PhD
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Chairperson)

Muhammad Rezal Kamel Ariffin, PhD
Associate Professor
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

Santo Banerjee, PhD
Fellow Researcher
Institute for Mathematical Research
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature:_____ Date:_____

Name and Matric No: Aliyu Danladi Hina, GS39910

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of
Chairman of
Supervisory
Committee: Assoc. Prof. Mohamad Rushdan MD Said

Signature: _____
Name of
Member of
Supervisory
Committee: Assoc. Prof. Muhammad Rezal Kamel Ariffin

Signature: _____
Name of
Member of
Supervisory
Committee: Dr. Santo Banerjee

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACI	Absolutely Continuous Invariant
BSC	Binary Symmetric Channel
BV	Bounded Variation
BER	Bit Error Rate
CDMA	Code Division Multiple Access
CSP	Constant Summation Property
Fig.	Figure
FPO	Frobenius Perron Operator
PSD	Power spectral density
PRNG	Pseudorandom number generator
PWLCM	Piecewise linear chaotic map
RNG	Random number generator
SS	Spread Spectrum
TRNG	True Random Number Generator
$\mathscr{B}$	σ-algebra of Borel sets
PDEs	Partial Differential Equations
λ	Lagrange Multiplier
$\mathcal{M}(f)$	Space of all probability measures of $\mathscr{B}$
LFSR	Linear Feedback Shift Register

CHAPTER 1

INTRODUCTION

1.1 Dynamical Systems

A dynamical system (DS) describes the evolution of a state over time. A DS contains the following two elements: (1) a set of possible states represented by one or more real variables, (2) a deterministic (not random or stochastic) rule that determines the present state from past states. The mathematical theory of dynamical system has its roots in classical mechanics, whose development commenced in the years XVI and XVII centuries by Galileo and Newton, respectively. The publication, "Principia" in the year 1689, by Newton laid down the mathematical principles of classical mechanics. This principles brought about the three laws governing the motion of bodies under the presence of external forces, describing the universal law of gravity. This inspired the work of mathematicians like Euler, Lagrange, Hamilton and Poincare that built on Newton's work.

A DS describes the passage in time of all points contained in a space I. The space I could be the space of states of some physical system. Mathematically I might be an Euclidean space or an open subset of Euclidean space or some other space such as a surface in $\mathbb{R}^n$. Given an initial position $X \in \mathbb{R}^n$, a dynamical system on $\mathbb{R}^n$ tells us where X is located after every one unit of time. At time zero, X is located at position X. If we measure the positions X_t using only integer time values, we have a discrete dynamical system. Otherwise time will be measured continuously with $t \in \mathbb{R}$, defining a continuous dynamical system.

The deterministic rule that determines the realization of successive points can be linear or non-linear. When it is non-linear we have a non-linear dynamical system (NDS) otherwise it is linear (LDS). The variables that describes the state of a DS are called the state variables. The set of all possible values of the state variables is the state space. The state space can be discrete, consisting of isolated points, such as if the state variables could only take on integer values. It could be continuous, consisting of a smooth set of points, such as if the state variables could take on any real value. In the case where the state space is continuous and finite-dimensional, it is often called the phase space, and the number of state variables is the dimension of the dynamical system.

1.1.1 Continuous-Time Dynamical Systems

This are dynamical systems in which the states takes values from the euclidean space $\mathbb{R}^n$ for $n \geq 1$. The states of a continuous-time dynamical systems (CDS)

are expressed as $x \in \mathbb{R}^n$. The CDS are given by ordinary differential equations (ODE) of the form:

$$\dot{x} = \frac{dx}{dt} = f(x) \tag{1.1}$$

where t stands for time, taking on real values, $x(t) : \mathbb{R} \to \mathbb{R}^n$ and $f : \mathbb{R}^n \to \mathbb{R}^n$ is the function that defines the ODE at time t, $x = x(t)$. The time t is represented by a continuum like $\mathbb{R}$ or $\mathbb{R}^+$. The equation (1.1) will have a solution. If it exist, it will be of the form $x(t) = [x_1(t), x_2(t), \ldots, x_n(t)]^T$ parametrized by a real variable $t \in \mathbb{R}$ valid on some given interval. The state space is (a subset of) $\mathbb{R}^n$, where the solutions live as parametrized curves, are called trajectories. Ordinary differential equations are examples of continuous dynamical systems (actually differentiable dynamical systems). Solving the ODE (finding the vector of functions $x(t)$), means finding the rule which stipulates any future state of a point $x(0)$ given a starting state.

The discovery of chaos was originally made with continuous-time dynamical systems, i.e., differential equations. An American mathematician and meteorologist,Edward Lorenz is one of the founders of chaos theory. He accidentally found chaotic behavior in the a model he developed called the Lorenz equations, with a view to study the dynamics of atmospheric convection in the early 1960s.

The Lorenz System:
First studied by Edward Lorenz (Lorenz, 1963), these systems of ordinary differential equations are notable for their chaotic behavior. The states: x is proportional to the rate of convection, y to the horizontal temperature variation, and z to the vertical temperature variation, Figure 1.1a.

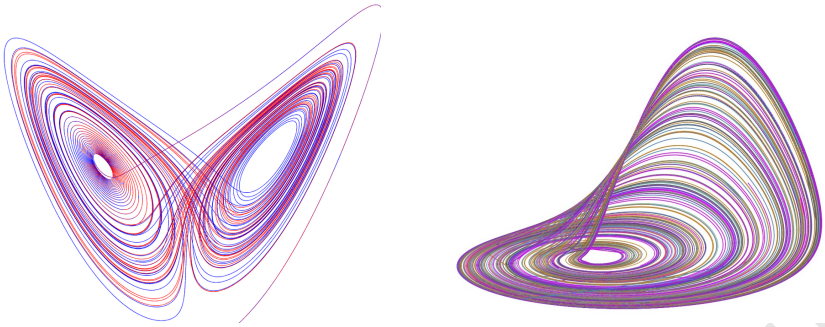
$$\begin{aligned} \dot{x} &= -\sigma(x - y) \\ \dot{y} &= x(\alpha - z) - y \\ \dot{z} &= xy - \beta z \end{aligned} \tag{1.2}$$

where $(\sigma, \alpha, \beta) = (10, 8/3, 28)$ are controlling parameters. This systems have been studied immensely for various purposes (Lü and Chen, 2002; Wang et al., 2010; Lu et al., 2002; Dar et al., 2010; Özkaynak and Özer, 2010).

Rössler **System:**
Rössler system was introduced by Otto *Rössler* in the 1970s (Rössler, 1976) as prototype equations with the minimum ingredients for continuous-time chaos. Its a systems of ordinary differential equations in three-dimensions.

$$\begin{aligned} \dot{x} &= -(y + z) \\ \dot{y} &= x + ay \\ \dot{z} &= bx + z(x + z) \end{aligned} \tag{1.3}$$

where a and b are parameters. The system of equations (1.3) is less in continuous chaos for at least three reasons: Its phase space has the minimal



(a) Lorenz System (b) *Rössler* System

Figure 1.1: Attractors of Continuous Systems

dimension three, existence of a linear term in the system thereby reducing its nonlinearity, and it generates a chaotic attractor with a single lobe, in contrast to the Lorenz attractor which has two lobes as can be seen in Figure 1.1b. The following references can be consulted among many others for detailed study (Chen and Yu, 1999; Ahmed et al., 2006; Sudheer and Sabir, 2011; Cafagna and Grassi, 2012). Because of the difficulties associated with the analytical study of continuous differential systems, a large amount of work has been devoted to dynamical systems whose state is known only at a discrete set of times.

1.1.2 Discrete-Time Dynamical Systems

Discrete-time dynamical systems (DDS), also called a map, are dynamical systems who's space I, is typically a compact continuum and the time is in $\mathbb{Z}$ or $\mathbb{N}$, taking on integer values. DDS are described by a difference equation of the form:

$$x_{n+1} = f(x_n) \tag{1.4}$$

The function f describes the evolution of the state x_n at time instant $n \in \{0, \mathbb{N}\}$ and is termed a mapping or simply a map. The sequence $\{x_n\}$ obtained by iterating equation (1.4) from an initial state x_0 is called the orbit of x_0, with $n \in \mathbb{N}$ or $n \in \mathbb{Z}$, depending on whether or not f is invertible.

Its only natural to restrict our study to discrete-time dynamical systems sharing some key properties with differential systems. It is often easy to extract discrete-time dynamical systems from a continuous-time system using the technique of Poincare sections. The initial conditions continuously determine the solution of a system of ODEs, so that continuous maps are singled out naturally. Invertibility is also a crucial property. Given an initial condition, the state of an ODE system can in principle be determined at any time in the future but also in the past; thus, we must be able to go backward in time. Maps satisfying these two requirements are called homeomorphisms (continuous maps with a continuous inverse). When this homeomorphisms are

differentiable along with their inverses, they define a class of maps called diffeomorphisms. A discrete time chaotic system is an iterated mapping, whose iteration number $n \in \mathbb{Z}$ is an integer. If we define the metric space (phase space) as I, then we have the following definition.

Definition 1.1 (Chen and Yu (1999)) *If for any $x \in I = [a, b]$ and $f : I \to I$, $n = 0, 1, \ldots$ the following holds: (a). $f^0 = x$, (b). $f^1 = f(x)$, (c). $f^n = f \circ f \circ f \circ \cdots \circ f(x)$ (n composition of f). The pair (I, f) defines the mapping that determines the state of the dynamics at discrete time intervals n.*

From the above definition we have, $f^n(f^m(x)) = f^{n+m}(x)$.

Definition 1.2 : *The sequence $\{f^n(x)\}_{n=0}^{\infty}$ is called the orbit or trajectory for the point x under the map f, defined to be*

$$\mathcal{O}(x_0) = \mathcal{O}^-(x_0) \cup \mathcal{O}^+(x_0) = \{x_n : n \in \mathbb{Z}\} \tag{1.5}$$

where $\mathcal{O}^-(x_0) = \{x_0, x_{-1}, x_{-2}, \ldots\}$ is called the backward trajectory and $\mathcal{O}^+(x_0) = \{x_0, x_1, x_2, \ldots\}$ is the forward orbit.

Maps are examples of discrete dynamical systems. Some examples of discrete dynamical systems include discretized ODEs and difference equations, time-t maps, and fractal constructions like Julia sets and the associated Mandelbrot arising from maps of the complex plane to itself. The number of distinct states defines the dimension of the map. Due to the deterministic and discrete nature of maps, their trajectories are always periodic or eventually periodic, with however long periods for a suitable choice of a controlling parameter. Discrete maps could be one dimensional as is the case of logistic, tent, Bernoulli, maps. Two dimensional like Henon, Baker and Ikeda maps etc. The following are some illustrations of discrete dynamical systems (maps):

- **One dimension (Logistic map)**
  The Logistic map is mathematically defined by:

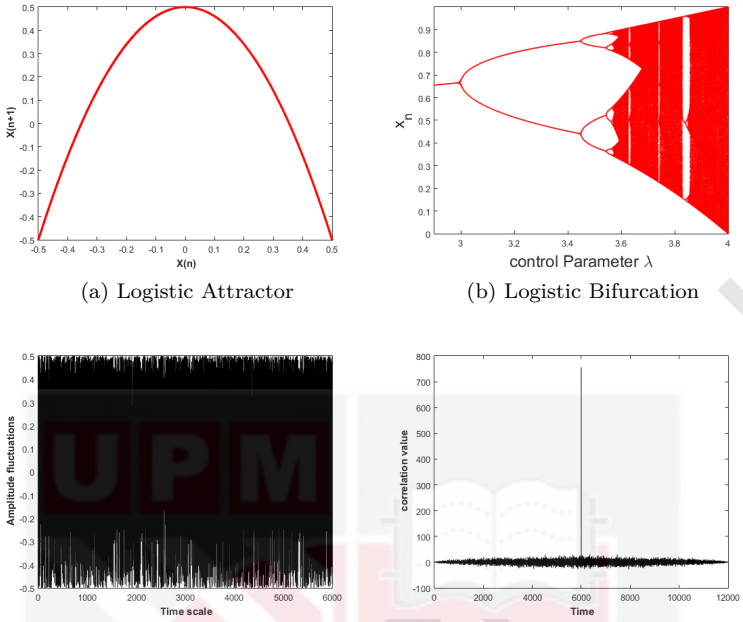
$$x_{n+1} = f(x_n) = \lambda x_n(1 - x_n) \tag{1.6}$$

  where $\lambda \in [0, 4]$ is the controlling parameter, and $x \in [0, 1]$.

- **One Dimensional (Tent Map)**
  The tent map is defined by:

$$x_{n+1} = f(x_n) = \begin{cases} \frac{x_n}{p} & \text{if } 0 \le x_n \le p \\ \frac{1-x_n}{1-p} & \text{if } p < x_n \le 1 \end{cases} \tag{1.7}$$

  where $f : I \to I$, and $I = [0, 1]$ and $p \in [0, 1]$.



(a) Logistic Attractor

(b) Logistic Bifurcation

(c) Amplitude fluctuations

(d) Autocorrelation

Figure 1.2: Attractor and Bifurcation diagrams of Logistic map.

- **One Dimensional (Chebyshev Map)** The Chebyshev map is defined by:

$$f(x_{n+1}) = \cos(k \cos^{-1}(x_n)) \tag{1.8}$$

where $x \in [-1, 1]$ and $k = 1, 2, \ldots$. It can also be presented in polynomial form of degree p,

$$T_{p+1}(x) = 2xT_p(x) - T_{p-1}(x) \tag{1.9}$$

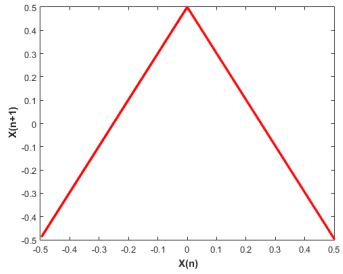
where $x \in I = [-1, 1]$, $p = 1, 2, \ldots$ and $T_0 = 1$, $T_1 = x$. The map has been used in many chaos based cryptographic proposals, (Kocarev and Tasev, 2003; Huang, 2012).

- **One Dimensional (Bernoulli (2-adic) Map)** The one-dimensional Bernoulli map is defined by:

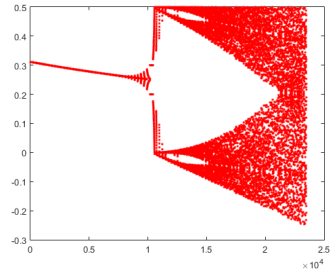
$$x_{n+1} = f_b(x_n) = 2x(mod\ 1) = \begin{cases} 2x_n & \text{if } 0 \leq x_n \leq 0.5 \\ 2x_n - 1 & \text{if } 0.5 < x_n \leq 1 \end{cases} \tag{1.10}$$

where $f_b : I \to I$, and $I = [0, 1]$. The stretching factor 2 in the equation (1.10) implies that the map has a global Lyapunov exponent of $log2$. The Bernoulli map is exact, which implies that it is both mixing and ergodic (to be discussed in the coming sections) (Driebe, 2013).

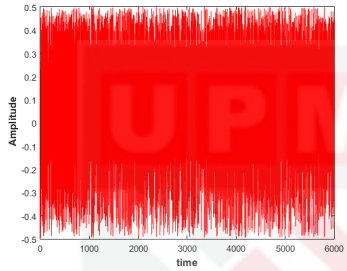
- **Two dimension (Henon Map)**



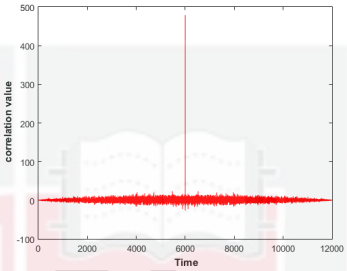
(a) Tent Attractor



(b) Tent Bifurcation



(c) Amplitude fluctuations



(d) Autocorrelation

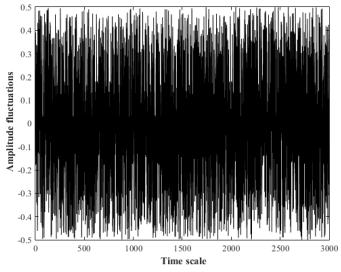
Figure 1.3: Attractor and Bifurcation diagrams of Tent map.

The Henon map is a widely used discrete time dynamical system which exhibits chaotic nature. It is found to be chaotic with values of the controlling parameters set at: $a = 1.4$ and $b = 0.3$. The map was first introduced by Michael Henon as shown in equation (1.11), (Hénon, 1976).

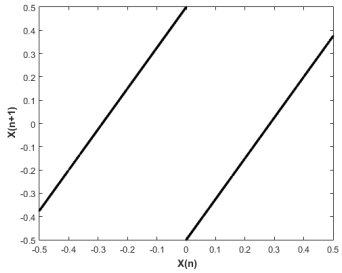
$$\begin{aligned} x_{n+1} &= a - x_n^2 + by_n \\ y_{n+1} &= x_n \end{aligned} \tag{1.11}$$

where a and b are controlling parameters. The mapping, equation (1.11), appears to have the same basic properties as the Lorenz (Hénon, 1976). The application of the two dimensional Henon map has gain its place in area of chaos based cryptography. In ciphers (Erdmann and Murphy, 1992; Li et al., 2001b; Khan et al., 2015), pseudorandom sequence generation (Zheng et al., 2008; Sun and Liu, 2009) image encryption (Soleymani et al., 2014; Belkhouche et al., 2004).

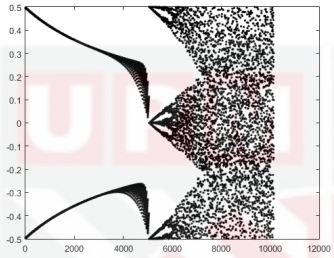
- **Two dimensional (Ikeda Map)**
  The Ikeda map: It was initially designed as a model for the movement of light around across a nonlinear optical resonator (Ikeda, 1979). It has been characterized with a bistable behavior; which makes it a good candidate for use in optical devices to obtain variable length pulses, infinite pulse trains, logical gate arrays and many more (Aboites et al.,



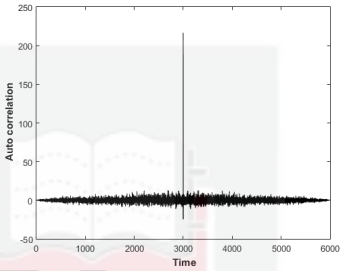
(a) Amplitude fluctuations



(b) Attractor



(c) Bifurcation



(d) Autocorrelation

Figure 1.4: Attractor and Bifurcation diagrams of the Bernoulli Map

2016). The simplified model is given by the equation (1.12):

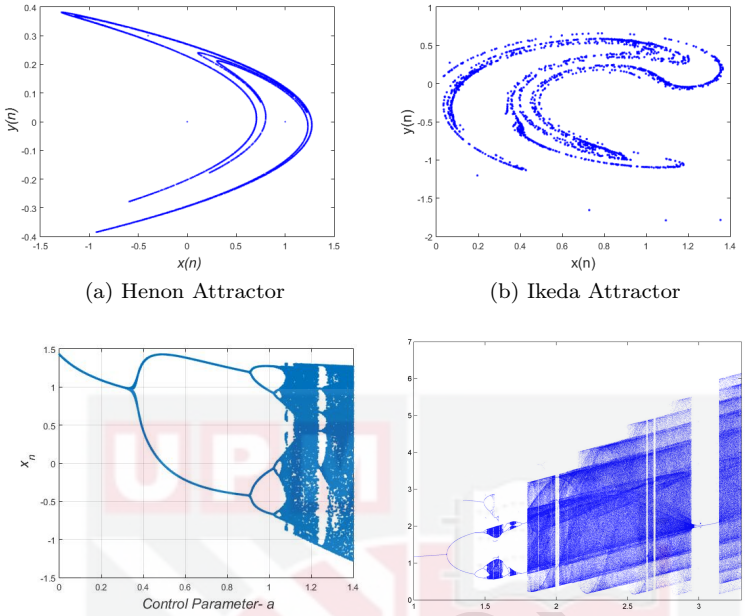
$$\begin{aligned} x_{n+1} &= 1 + \alpha(x_n cost_n - y_n sint_n) \\ y_{n+1} &= \alpha(x_n sint_n + y_n cost_n) \end{aligned} \tag{1.12}$$

where $t_n = 0.4 - \frac{6}{1+x_n^2+y_n^2}$ and α is a controlling parameter for which the map is chaotic for all $\alpha \geq 0.6$. It has been used quite reasonably in a number of cryptographic applications (Jia, 2010; Cao, 2013; Kaur and Sharma, 2013; Candido et al., 2015).

Many other two dimensional (2D) maps like the Baker map, Kaplan-yorke map etc can be found in the literature.

The chaotic property known to dynamical systems is its important feature. This feature is what makes such systems appealing for cryptography. Upon satisfying the following conditions, a systems is said to be chaotic:

- Exponential sensitivity to initial conditions by the system trajectories.
- In a given interval of frequencies, the system has continuous spectral concentration .



(a) Henon Attractor (b) Ikeda Attractor

(c) Henon Bifurcation (d) Ikeda Bifurcation

Figure 1.5: Phase and Bifurcation diagrams of 2D maps.

- Information about the initial value of the system is lost exponentially.

However meeting this conditions is rather hard, thus a metric that is usually used as a measure of chaos is a value called the Lyapunov exponent.

1.2 Chaotic Dynamical System

The apparent random behavior exhibited by a deterministic system under deterministic conditions is referred to as Chaos. As the study of chaos gets in-depth, one soon realizes chaos cannot be defined with a single precise definition. However, for a chaotic phenomena, there must be transitivity and sensitive dependence to initial conditions.

Given a map $f : I \to I$, if for any open sets $U, V \in I$ there exist a $k > 0$ such that $f^k(U) \cap V \neq \emptyset$, it is said to be transitive. Transitivity means that given a point in some arbitrary small neighborhood of the attractor, it will on the course of its journey, visit all other regions of the attractor under the action of the map f.
The map f is said to exhibits sensitive dependence on initial conditions if there exists an $t > 0$ such that for any $x \in I$ and any neighborhood B of x there exists a $y \in B$ and $n \in \mathbb{N}$ such that $|f^n(x) - f^n(y)| > \epsilon$ (Devaney, 2008).

There are two kinds of definition of chaos: Topological and Measure theoretical definitions. In the topological sense of the definition of chaos, we have the following attributed to Robert Devaney:

Definition 1.3 *[Devaney, 2008]: Let I be a metric space. A map $f : I \to I$ is said to be chaotic if:*
1. f is transitive: for all non-empty subsets $V, U \in I$ there exist a k such that $f^k(V) \cap U \neq \emptyset$.
2. The set of periodic point of f are dense in I.
3. f has sensitive dependence to initial conditions.

Unpredictability in dynamical systems is ensured by Sensitivity to initial conditions, whereas indecomposability is reflected in its topological transitivity, meaning, there does not exist a partition of the domain of the map describing the system such that the map is surjective on the disjoint sets in the partition (Driebe, 2013). The Devaney's definition of chaos is the widely known and accepted definition. However, a measure theoretic approach to the definition has also been given by Li & Yorke (Li and Yorke, 1975).

Definition 1.4 *[Li and Yorke, 1975]: A map $f : I \to I$ on a compact metric space (I, d) is called chaotic in the sense of Li and Yorke – if there exists an uncountable subset S (called a scrambled set) of I with the following properties:*
1. $\lim_{n\to\infty} \sup d(f^n(x), f^n(y)) > 0$ *for all* $x, y \in S$, $x \neq y$,
2. $\lim_{n\to\infty} \inf d(f^n(x), f^n(y)) = 0$ *for all* $x, y \in S$, $x \neq y$,
3. $\lim_{n\to\infty} \sup d(f^n(x), f^n(p)) > 0$ *for all* $x \in S$, $p \in I$, *p-periodic.*

Devaney chaos and Li York chaos are interrelated via topological entropy. Devaney chaos implies positive topological entropy and the converse is not true. Positive topological entropy implies Li Yorke chaos and here too the converse does not hold. According to the law of transitivity in analysis Deveney chaos implies Li Yorke chaos. On the interval map Deveney chaos is the strongest whereas Li Yorke's chaos is the weakest.

Having established the existence of chaos, the measure of the degree of chaos of a given map is important as determining its existence. Quantitative study of chaos is motivated by the following: The need for some quantitative test that can distinguish chaotic behaviour from noisy behaviour (due to random external influences). Secondly, the need for some quantitative measure of the degree of chaos which demonstrates how chaotic behaviour changes with the system parameter(s) (ElShaarawy and Gomaa, 2014).

1.2.1 Quantification of Chaos

Systems when Chaotic are said to be unpredictable, but the question is to what extend? how do we know the degree of chaoticity of a system? How can we say that one system is more chaotic than another? Simulations and visualizations of chaotic attractors showed that they come in many shapes and forms and have distinct properties, such as being fractals and having sensitive dependence on initial conditions. Notable among various tools used to distinguish between chaotic and non-chaotic evolution, is the largest Lyapunov exponent. It is probably the most commonly used. However, the largest Lyapunov exponent will not work alone, because in many cases largest Lyapunov exponent is positive for unstable systems too. Combined analysis of bifurcation diagram and largest Lyapunov exponent gives clear picture about chaos analysis. From bifurcation diagrams, we can see if Lyapunov exponent is positive, during which we say the oscillations are chaotic otherwise not. Remember this can be one way valid in one situation. There can be other approaches valid in other scenarios. Among other measures we have correlation dimension, Dense Filled phase space and Poincare Section. Attractors do not include other attractors within them, that is they have to be minimal set. Given an attractor with a positive Lyapunov exponent, then it is said to be a chaotic attractor. For cryptographic purposes, dynamical system used in cryptographic algorithm design, are expected to be ergodic and mixing.

• **Ergodicity:** Ergodicity is related to concept of folding and mixing. With an ergodic system, almost every trajectory will densely cover the phase space of the system. There are many different formal definitions of ergodicity, we should however note that all the definitions are completely equivalent. The idea of ergodicity arises if we have only one sample function of a stochastic process, instead of the entire ensemble.

Definition 1.5 *The system $(\mathcal{I}, f)$ is ergodic when for any invariant set $f(I) = I$ the measure $\mu(I) = 0, 1$, for $I \in \mathcal{I}$.*

The implication of this definition is that, the trajectory starting from any point is never bounded in some subset of the space, thus therefore for analysis, the whole space will have to be considered.
Ergodicity refers to that property of a system to the same behavior when averaged over time or space (Alligood et al., 2008). Time average are taken generally over one experiment, while space averages are determined over many experiments at a given parameter value and different initial conditions. For a continuous system $F(x)$, its average over time is given by:

$$F(x) = \lim_{N\to\infty} \frac{1}{N} \int_0^N F(x(t))dt. \tag{1.13}$$

A weighted invariant probability density function will be required when defining space average. This invariant density function is calculated by the use of

an invariant measure. The probability density function, $\rho(x)$, maps the phase space of the dynamical system into intervals and determines the probability of an interval containing the variable x. Given a sub-interval ΔI and a measure μ, the probability of a variable x contained in ΔI, $\mu(\Delta I)$ is given by:

$$\mu(\Delta I) = \int_{\Delta I} \rho(x)dx = \int_{\Delta I} d\mu(x) \tag{1.14}$$

If the measure is known, it is possible to find the average of a function F(x) giving the following equation of the dynamics averaged over the space of the function

$$F(x) = \lim_{N\to\infty} \int_0^N F(x)\rho(x)dx = \int_0^N F(x)d\mu(x). \tag{1.15}$$

A system that equates the equations (1.13) and (1.15):

$$F(x) = \lim_{N\to\infty} \frac{1}{N} \int_0^N F(x(t))dt = \int_0^N F(x)d\mu(x) \tag{1.16}$$

is said to be ergodic. Therefore, taking the average of infinite time along an orbit is equal to using the measure of averaging the points in an orbit.
It is the property of ergodicity which ensures that each interval of the chaotic attractor in a chaotic system will be visited continuously as the number of iterations of an initial condition approaches infinity. In a chaos-based cryptosystem, realizing this property will differ based on the architecture of the cryptosystem.

Definition 1.6 : *Given the mapping $F : I \to I$, any invariant set A of the mapping F, and a measure μ, then F is ergodic with respect to the measure μ if $\mu(A) = 0$ or 1. In other words: Given the measurable subsets $A, B \subset I$ the system (f, I, μ) is ergodic if the following holds:*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} \mu\Big(f^{-j}(A) \cap B\Big) = \mu(A)\mu(B). \tag{1.17}$$

A single sample function will often provide little information about the statistics of the process. However, if time averages equal ensemble averages, (ergodic process), one sample function is enough to derive all statistical information required, such that the sample function represents the entire process. We should note that process must necessarily be stationary for this to occur. Thus ergodicity implies stationarity. There are levels of ergodicity, just as there are levels (degrees) of stationarity. We present two levels of ergodicity; ergodicity in the mean and ergodicity in correlation
Ergodicity in the mean: A process is ergodic in the mean if

$$\bar{x}_t = \lim_{t\to\infty} \frac{1}{T} \int_0^T x_t dt = \langle x_t \rangle \tag{1.18}$$

Therefore, ergodicity of the mean implies stationarity of the mean, however, the converse is not true.
Ergodicity in the autocorrelation: A process is ergodic in the autocorrelation if

$$C_x(f) = \bar{x}_t x_{t+\tau} = \lim_{t\to\infty} \frac{1}{T} \int_0^T x_t x_{t+\tau} dt = \langle x_t x_{t+\tau} \rangle \tag{1.19}$$

In cryptographic point of view, this phenomena makes the use of chaotic systems/maps for cryptographic applications possible.

• **Mixing:** Given any arbitrary initial point, its ability to reach any subset of the phase space $\mathcal{I}$ is guaranteed by the mixing property, with probability proportional to the size of that subset in the state space.

Definition 1.7 *The system $(\mathcal{I}, f)$ has the mixing property if $f : \mathcal{I} \to \mathcal{I}$ is the measure preserving mapping, and for each pair of sets $A, B \in I \subset \mathcal{I}$ with nonzero measure μ the following is satisfied:*

$$\lim_{n\to\infty} \mu(A \cap f^n(B)) = \mu(A)\mu(B). \tag{1.20}$$

A map is called mixing if any smooth initial probability density $\rho(x)$ converges to the invariant measure $\mu(x)$ after a good number of successive iterations. Mixing, which is a stronger requirement that ergodicity is not easy to prove for a given map. Let $\phi_1(x)$ and $\phi_2(x)$ be two integrable functions, the generalized correlation function for the map f is given by

$$C(\ell, \phi_1, \phi_2) = \lim_{J\to\infty} \frac{1}{J} \sum_{j=0}^{J-1} (\phi_1(x_{j+\ell})\phi_2(x_j) - \langle \phi_1 \rangle \langle \phi_2 \rangle) \tag{1.21}$$

where

$$\langle \phi_i \rangle = \lim_{J\to\infty} \frac{1}{J} \sum_{j=0}^{J-1} \phi_i(x_j), \quad i \in \{1, 2\} \quad \forall\ i. \tag{1.22}$$

If for any of the functions ϕ_1 and ϕ_2,

$$\lim_{\ell\to\infty} C(\ell, \phi_1, \phi_2) = 0 \tag{1.23}$$

the map is said to be mixing.

• **Lyapunov Exponent:** Sensitivity of the dynamical behavior of a system when its initial state is perturbed by a small amount is an important feature of chaos, It measures the degree of chaos. Nearby points in the phase space separate fast (say exponentially with time), over most of the phase space, then the system can reasonably be described as being dynamically unstable. The Lyapunov Exponent (LE) λ is a value determined from the following: Given

the map:

$$x_{n+1} = f(x_n) \tag{1.24}$$

Let (x_0^1, x_0^2) be a pair of initial points in the phase space $I \subset \mathbb{R}$ such that

$$x_n^1 = f^n(x_0^1), \quad \text{and} \quad x_n^2 = f^n(x_0^2). \tag{1.25}$$

If these points separate exponentially with increasing n,

$$|x_n^1 - x_n^2| = |x_0^2 - x_0^1| * e^{\lambda n}, \quad where \quad (\lambda > 0).$$

For a large n, $(1/n)ln|x_0^2 - x_0^1| \to \lambda$. If we allow the limit $\delta_0 = |x_0^2 - x_0^1| \to 0$, then:

$$\begin{aligned} \lambda &= \lim_{n\to\infty} \frac{1}{n} \lim_{\delta_0 \to 0} \ln \left| \frac{x_n^1 - x_n^2}{x_0^2 - x_0^1} \right| \\ &= \lim_{n\to\infty} \frac{1}{n} \lim_{\delta_0 \to 0} \ln \left| \frac{f^n(x_0^1) - f^n(x_0^2)}{x_0^1 - x_0^2} \right| \\ &= \lim_{n\to\infty} \frac{1}{n} \ln \left| \frac{df(x_0^1)}{dx} \right| \end{aligned} \tag{1.26}$$

from

$$\frac{df^m(x_0)}{dx} = \prod_{i=0}^{n-1} \frac{df(x_i)}{dx_i},$$

we have for a particular trajectory τ:

$$\lambda_\tau = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{df(x_i)}{dx_i} \right|$$

the Lyapunov exponent for the trajectory τ. For a spectrum of initial conditions asymptotically attracted to the same ergodic subset of the phase space, then their Lyapunov exponents will all be the same, thus we have:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \frac{df(x_i)}{dx_i} \right|. \tag{1.27}$$

• **Correlation Dimension:** The complexity of chaotic signals can be described by a parameter D_2 known as "correlation dimension. (Michalak, 2014). It has been a powerful indicator for the description of the fractal structure of invariant sets in dynamical systems, in addition to instruments like the Lyapunov exponents and the entropy. Reliable estimates of D_2 can be obtained with relatively short time series as reported by Theiler et. all (Theiler, 1987). This puts D_2 ahead of Lyapunov exponents and entropy due to their challenging nature of computations. Let us denote $x_1, x_2, x_3, \ldots, x_n$ the set of n-dimensional real valued data points lying on a chosen chaotic attractor. Following the algorithm, we define the correlation sum $C(r)$ as (Grassberger

and Procaccia, 2004):

$$C(r) = \frac{2}{n(n-1)} \sum_{i=1}^{n} \sum_{j=i+1}^{n} \Theta(r - ||x_i - x_j||) \tag{1.28}$$

where $||\cdot||$ computes the Euclidean distance, n is the number of the data points, $\Theta(\cdot)$ is called the Heaviside function such that $\Theta(x) = 1$ for $x > 0$ and 0 otherwise. The equation (1.28) computes number of pairs of given data points whose distance is less than some given radius $r > 0$, normalized by the total number of pairs. Correlation dimension D_2 is therefore defined by:

$$D_2 = \lim_{r \to \infty} \lim_{n \to \infty} \frac{\partial ln(C(r))}{\partial ln(r)} \tag{1.29}$$

More details on correlation dimension can be found in (Theiler, 1987; Grassberger and Procaccia, 2004; Ding et al., 1993).

1.2.2 The Chaotic Maps

Chaotic maps are discrete time dynamical systems that are generally defined with recurrence relations as shown below:

$$x_{n+1} = f(x_n), \tag{1.30}$$

where $x \in I \subset \mathbb{R}^n$, and $f : I \to I$ is an n-dimensional difference function, with n as the number of distinct states which defines the dimension of the map. As discussed in previous sections, these maps could be of one dimension (1D), two dimension (2D) or even three dimensions(3D). While continuous time flows can only be chaotic at dimension three, discrete maps are chaotic at dimension one. One will be able to produce a very complex behavior with a one dimensional map.

The choice of 1D maps is based on the fact that their dynamics are comparatively well understood, for example, their probability density functions can be derived mathematically, they are widely used for the design of chaos based Cryptosystems (Phatak and Rao, 1995; Shujun et al., 2001; Addabbo et al., 2004, 2005). Hence, one-dimensional chaotic maps are herein focused upon. These maps are required to meet some conditions before they are considered good candidates for cryptography:
1. The map $x_{n+1} = f(x_n)$ is a surjective map defined on an interval $I = [a, b]$,
2. $x_{n+1} = f(x_n)$ is ergodic on I with a unique invariant density function $\rho(x)$,
3. $\rho(x)$ is even-symmetrical to $x = \frac{(a+b)}{2}$,
4. x_n for $n \to \infty$ is dense in I.

There are other kinds of 1D maps which do not have periodic windows (except the Logistic map) and consequently they do not produce periodic signals once in the chaotic region. These 1D chaotic maps are known as piecewise linear

maps. Examples of these maps are Bernoulli and Tent maps.
A map $f : I \to I$ is called a piecewise monotonic map if it satisfies the following properties:
1. The interval I can be partitioned into $a = d_0 < d_1 < d_2 < \cdots < d_{N_f} = b$ such that for each $i = 1, 2, \ldots, N_f$, $(N_f \geq 2)$, f_i (the restriction of f to the interval $[d_{i-1}, d_i)$, $1 \leq i \leq N_f$) is a C^2 function.
2. f_i is onto, $(f([d_{i-1}, d_i)) = [a, b])$
3. f has a unique absolutely continuous invariant (ACI) measure denoted by $\rho^*(x)dx$ (Condition under which f satisfies the ACI appears in (Boyarsky and Scarowsky, 1979)). A class of these maps satisfies the property:

$$|g_i'(x)|\rho^*(x) = \frac{1}{N_f}\rho^*(x), \quad i = 1, 2, \ldots, N_f \tag{1.31}$$

where $g_i(x) = f_i^{-1}(x)$, $\rho^*(x)dx$ the ACI measure. Maps that are found to satisfy equation (1.31), referred to as an (EDP) includes the following: the logistic map, the tent map, R-adic map, the Chebyshev map of degree k, where $N_f = 2, 2, R, k$, respectively. These 1D maps are commonly used for the design of chaos based cryptosystems (Wah, 2007). In this thesis we will be considering only maps called piecewise monotonic maps, the class of 1D maps that satisfies what is called the equidistributivity property (EDP).

1.2.3 Equidistributivity Property (EDP) of 1D Chaotic Maps

Given a piecewise-monotone onto map $f(x)$, it is said to satisfy the the equidistributivity property (EDP) if equation (1.31) holds. If we let the interval I be partitioned into I_0 and I_1 such that $I = I_0 \cup I_1$ and $I_0 \cap I_1 = \emptyset$. Thus therefore as contained in (Kohda, 2004), the binary sequence generated by a threshold function $\Theta_t(x)$ defined on the sub-intervals I_0 and I_1 generates a sequence of i.i.d binary random variables.
If for a class of maps that satisfy the EDP and an L_1, say, H, the following holds true:

$$\langle H \rangle = \frac{1}{N_f}\sum_{i=1}^{N_f} H(g_i(x)) \tag{1.32}$$

Then H is said to satisfy the constant summation property (CSP).

Definition 1.8 *The Frobenius-Perron operator (FPO) $\mathcal{L}_f$ acting on the function of bounded variation $H(x) \in L^\infty$ for $f(x)$ is defined as*

$$\mathcal{L}(H(x)) = \frac{d}{dx}\int_{f^{-1}([a,x])} H(z)dz = \sum_{i=1}^{N_f} |g_i'(x)|H(g_i(x)) \tag{1.33}$$

where $g_i(x) = f_i^{-1}(x)$ is the i-th pre-image of x.

(Lasota and Mackey, 2013) reports that $\mathcal{L}_f$ is the evolution operator of the probability density function under the map $f(\cdot)$. Since the notion of the map f on which the evolution operator is well understood, we will henceforth write $\mathcal{L}_f$ as $\mathcal{L}$. We should note that the ACI measure satisfies the FP equation: $\mathcal{L}\rho^* = \rho^*$.

A sufficient condition has been introduced by (Kohda and Tsuneda, 1997) on the generation of i.i.d. sequences. If the binary functions B_i where (B_1 is as in equation (3.3) and B_2 as in equation (3.4)) satisfy:

$$\mathcal{L}\{B_i(x)\rho^*(x)\} = \langle B_i\rangle\rho^*(x), \quad x \in I \tag{1.34}$$

Then the sequence $\{B_i(x_n)\}_{n\geq 0}$ is an i.i.d. sequence. (Kohda and Tsuneda, 1997) equally points out that if the map $f(x)$ and its measure are (even) symmetrical, $f(x)$ satisfies (EDP) and the functions B_i satisfies the symmetry property:

$$B_i(a+b-x) = 1 - B_i(x), \quad x \in I = [a,b] \tag{1.35}$$

then the equation (1.34) holds true implying that $\{B_i(x_n)\}_{n\geq 0}$ is i.i.d. We will be concerned with maps that satisfies what is refereed to as the symmetric properties of invariant measure: $\rho^*(a+b-x) = \rho^*(x)$ for all $x \in I$. With such maps, $\langle B_i\rangle = \frac{1}{2}$. These sequences will be generated from amongst the class of maps satisfying the EDP property. In any case, there has to be an established relationship between these maps such that the choice the map will be invariant. Thus the sequences generated will be of same statistical qualities. Such maps are said to be topologically conjugate.

1.2.4 Topological Conjugacy between 1D Chaotic Maps

We will here put forward justification of the equivalence of any two given maps within the class considered (piecewise monotonic maps), using topological conjugacy.

Definition 1.9 *Two maps (Topological spaces) $f_x\colon I \to I$ and $g_k\colon J \to J$ where $x \in I = [0,1]$ and $k \in J = [0, 2^n - 1]$, are said to be topologically conjugates if there exist a continuous and invertible map with continuous inverse h, such that: $h\colon I \to J$, $y = h(x)$, and*
$f(x) = h \circ g \circ h^{-1}(x)$, $g(y) = h^{-1} \circ f \circ h(y)$.

Let $h\colon I \to J$ be a conjugacy that satisfies: $h \circ f = g \circ h$ or $h(f(x)) = g(h(y))$. If we consider the orbit of (x_0) under $f : \{x_0, x_1 = f(x_0), x_2 = f^2(x_0), \dots\}$. We can find (x_0) under h such that $h(x_0) = y_0$ and define its orbit under g as:$\{y_0, y_1 = f(y_0), y_2 = f^2(y_0), \dots\}$. These two orbits are therefore equivalent under h, that is $y_i = h(x_i)$ for all $i \geq 0$.
This conjugacy can be extended to the iterate f^n and g^n of the two maps with $f^n \circ h(y) = h \circ g^n(y)$ such that $f^n(x) = h \circ g \circ h^{-1}(x)$, $g^n(y) = h^{-1} \circ f \circ h(y)$.

If f is n-circle periodic ($f^n(x) = x$) so is g ($g^n(y) = y$), since it can be verified that: $h(f^n(x_0)) = g^n(h(x_0))$

$$\begin{aligned} g^n(h(x_0) &= g^{n-1}(g(h(x_0))) = g^{n-1}(h(f(x_0)) \\ &= g^{n-2}(g(h(f(x_0)))) = g^{n-2}(h(f^2(x_0)) \\ &\vdots \\ &= g^{n-m}(h(f(x_0)) \\ &\vdots \\ &= h(f^n(x_0)) \end{aligned} \tag{1.36}$$

Reversing from J and g to I and f follows the same procedure utilizing h^{-1}. If h is onto, then h is a factor map, and hence there is a topological semi-conjugacy from f to g. If h is one-to-one, then h is an embedding. If h is an onto embedding, then it is a topological conjugacy.

If f and g are topologically conjugate via a homeomorphism h as given above, then f^n and g^n are also topologically conjugates via h. The implication of this statement is that the equilibria of the conjugate maps, ordered on the line, can be put into one-to-one correspondence and have the same sink, source or semi-stability. This one-to-one correspondence enables us to derive the trajectory of one map from the other provided they are topologically conjugate.

We will wish to achieve in systems of lowest dimension, the most important aspect of chaos: "chaotic behavior". Thus, we would like to reduce as much as possible the dimension of state space. However, this conflicts with the requirement of invertibility. On the one hand, it can be shown that maps based on a one dimensional homeomorphism can only display stationary or periodic regimes, and hence cannot be chaotic. However, since invertibility is not a dire requirement, it can be traded off, thereby introducing singularities. One-dimensional (1D) chaotic systems are easily found. It is, in fact, no coincidence that chaotic behavior appears in its simplest form in a non-invertible system. As emphasized in the book by (Gilmore and Lefranc, 2012), singularities and non-invertibility are intimately linked to the mixing processes (stretching and folding) associated with chaos.

1.3 Cryptography

Cryptography is the process of converting ordinary plain text (message, information) into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process. Cryptography not only protects data from theft or alteration, but can also be used for user identification and authentication. Traditionally, cryptography was effectively synonymous with encryption and decryption, but of recent, cryptography is mainly based on mathematical the-

Table 1.1: Comparison between Chaos and Cryptography

Chaos	Cryptography	Description
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial condition/parameter	Diffusion with small changes in plaintext/secret key	Small deviation in the input causes large change in the output
Topological Mixing	Diffusion with small changes in one plain block of the whole Diffusion with small changes in one plain block of the whole plaintext	Small deviation in the local area causes a large change in the whole space.
Deterministic Dynamics	Deterministic pseudorandomness	A deterministic process can cause random-like (pseudorandom) behaviour
Structure Complexity	Algorithmic (Attack) Complexity	A simple process has a very high complexity

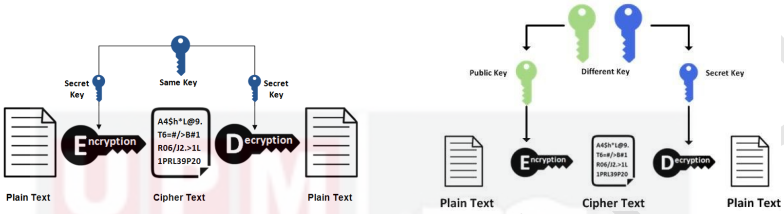
ory and computer science practice applied in many applications. These applications includes banking transactions cards, computer passwords, e-commerce transactions etc.

Cryptography was initially developed for the purpose of protecting security of all secret information relating to military and government organizations. It has developed to be an indispensable tool used in protecting information in modern digital society. Cryptology, which is the combination of cryptography and cryptanalysis (the science of analyzing and breaking cryptographic codes), is the science that aims to provide information security in the digital world. Confidentiality, authentication and data integrity during communication services such as email, banking or online shopping are derived from Cryptographic techniques. Confidentiality is keeping the information secret from unauthorized access while authenticity ensures that data have not been modified by an unauthorized user (data integrity), and also verifies who the author of the data is (data origin authentication).
Cryptography is the study and design of algorithms and protocols with a view to achieve information security whereas Cryptanalysis is the study of mathematical techniques that attempt to break cryptographic primitives. Cryptographic algorithms are usually split into two families, symmetric algorithms, asymmetric algorithms and hash functions.

Symmetric algorithms (secret key algorithms) require that the same secret key is shared by the communicating parties (eg, RC4, RC6, Blowfish etc). Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side

the receiver applies the same key to decrypt the message and recover the plain text, Figure 1.6a.

In asymmetric key algorithms (public key algorithms), the public key is made public, and the corresponding private key is kept secret by a single entity. In Public-Key Cryptography (eg. Diffie-Hellman, RSA, Elliptic Curve), two related keys (public and private key) are used. Public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and the private key for decryption, Figure 1.6b.



(a) Asymmetric (b) Symmetric

Figure 1.6: Kinds of cryptographic Algorithm

Cryptography is today referred to the science and art of transforming information into an unintelligible manner such that an unauthorized person will not make any sense out of it. Such transformation makes the message immune and secure against attacks. As against the traditional understanding of cryptography as just been the idea of encryption and decryption, today it involves three distinct mechanisms viz: symmetric key encryption, asymmetric key encryption and hashing.
In the traditional context of cryptography, a message M is encrypted by a sender A, using an encryption key E_k to produce a ciphertext C. This ciphertext C is then transmitted through an insecure channel to the recipient B. B then uses a decryption key D_k to recover back the original message sent. If a symmetric cryptographic algorithm is deployed, $k_e = k_d$ an example of such is the stream ciphers, whereas for asymmetric algorithms, $k_e \neq k_d$ with the public key cryptosystem RSA as an example. Encrypting the message M to generate the ciphertext C and decrypt C to get back M:

$$C = E_k(M), \quad \text{and} \quad M = D_k(C), \tag{1.37}$$

1.3.1 Conventional Cryptography

Cryptography, is the art and science that encompasses the principles and methods of transforming an intelligible message (plaintext - M) into an unintelligible one (ciphertext - C) through a process called encryption (enciphering - E). The ciphertext (C) is then re-transformed back to the original message (M) through another process called decryption (deciphering - D). The algorithm that is responsible for both enciphering/deciphering is called a cipher. Figure (1.7) depicts an encryption and decryption scheme in which a sender

A send encrypts a message using a key and sends the ciphertext to receiver B. B then decrypts using the key to recover back the original message sent by A. It shows a generalized description of a cryptosystem (Stinson, 2005).

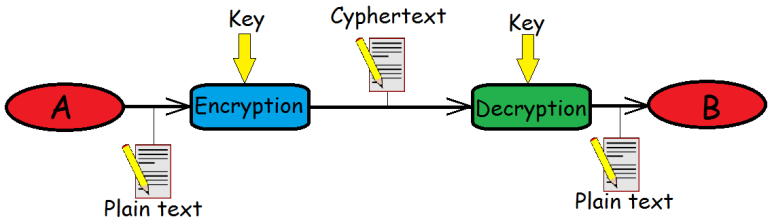


Figure 1.7: Encryption and Decryption

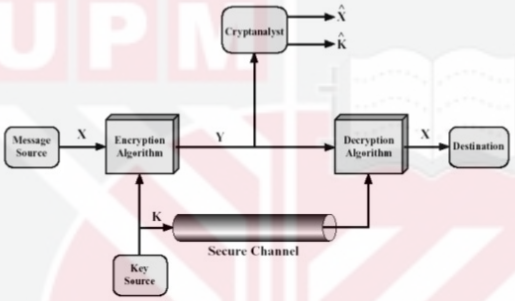


Figure 1.8: A generalized Model of a Cryptosystem

A Cryptosystem is a combination of cryptographic algorithms (symmetric, asymmetric, hashing). It is a protocol for communicating with both confidentiality and authenticity. To achieve confidentiality, chose/generate a random symmetric key, Encrypt your message with that key and then encrypt the key using the recipient's public key. The recipient can then decrypt first the symmetric key, and then the message. Only they will be able to do so, provided that their private key is kept secret.
To achieve authenticity, compute a digest of your message using a cryptographically secure hash function. Encrypt this digest using your private key to produce the signature. When the recipient receives the message, they will be able to compute the digest themselves, and then decrypt your signature with your public key. If the answers are the same, then they have confidence that the message came from you and was not altered, provided that you've kept your private key secret. The four principles of cryptography are:

- Confidentiality: This refers to a set of rules that limits access or adds restriction on certain information.
- Data Integrity: It takes care of the consistency and accuracy of data during its entire life-cycle.

- Authentication: This confirms the truth of an attribute of a datum that is claimed to be true, sent by some entity.
- Non-Repudiation: This ensures the inability of an author of a statement resp. a piece of information to deny it.

1.3.2 Kinds of Ciphers

A cipher simply put, is a set of steps (an algorithm) for performing both an encryption, and the corresponding decryption. All ciphers involve either transposition or substitution, or a combination of the two operations. If the elements of the plaintext (e.g., a letter, word, or string of symbols) are rearranged without any change in the identity of the elements, such a cipher is called a transposition cipher. In substitution ciphers, elements are replaced by other objects or groups of objects without distorting their sequence. Cipher devices or machines have commonly been used to encipher and decipher messages.
The first cipher device appears to have been employed by the ancient Greeks around 400 bc for secret communications between military commanders. This device, called the "scytale", consisted of a tapered baton around which was spirally wrapped a piece of parchment inscribed with the message. When unwrapped the parchment bore an incomprehensible set of letters, but when wrapped around another baton of identical proportions, the original text reappeared. Other examples of ancient ciphers includes: The Caesar Cipher and the *Vigenère* Cipher.

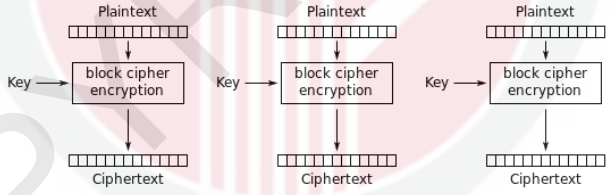


Figure 1.9: Electronic Codebook (ECB) Mode

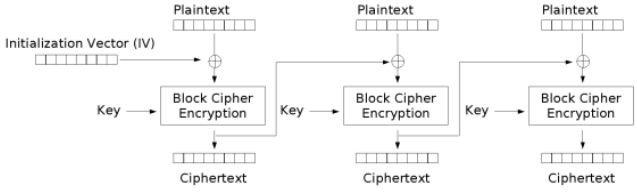


Figure 1.10: Cipher Block Chaining (CBC) Mode

• **Block Ciphers:**
Block ciphers encrypt blocks of fixed sizes through some simple operations and

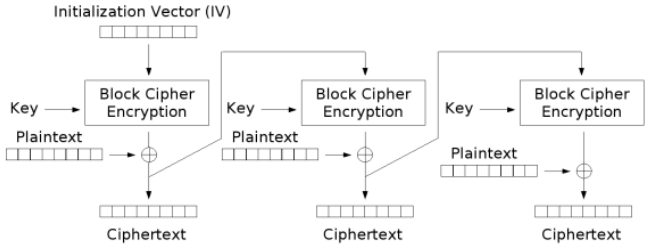


Figure 1.11: Cipher Feedback (CFB) Mode

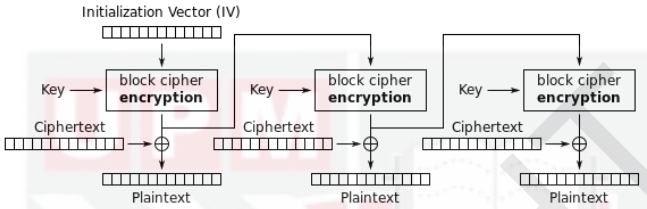


Figure 1.12: Output Feedback (OFB) Mode

some kind of feedback mechanisms. Some applications need to parallelized encryption or decryption, while others need to be able to pre-process as much as possible.
The error propagation phenomenon implies that errors in the encrypted text produce errors in the decrypted plaintext. So, it is important that the decrypting process be able to recover from bit errors in the ciphertext. The most popular block ciphers includes among others the DES, 3DES, AES, Blowfish, twofish etc.
The modes of operation of block ciphers are configuration methods that allow those ciphers to work with large data streams, without the risk of compromising the provided security. These configurations called the block cipher modes of operations, includes: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Output Feedback (OFB). These modes of operations are illustrated in Figs. 1.9 through 1.12.

• **Stream Ciphers:**
A stream cipher is an encryption algorithm that encrypts one bit or byte of plaintext at a time. It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure, its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad. RC4, which stands for Rivest Cipher 4, is the most widely used of all stream ciphers, particularly in software. It's also known as ARCFOUR or ARC4. RC4 has been used in various protocols like WEP and WPA (both security protocols for wireless networks) as well as in TLS. Unfortunately, recent studies have revealed vulnerabilities in RC4, prompting Mozilla and

Microsoft to recommend that it be disabled where possible.

1.4 Chaos Based Cryptography

Chaos has created itself a niche in cryptography. It has emerged as a potential solution to many problems due to the following fundamentals of chaotic systems: (a) determinism; and (b) sensitive dependence on initial conditions. Since 1990s, many researchers have noticed that there exists an interesting relationship between chaos and cryptography: many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems, as shown in table 1.2. Chaos provides greater diversity in terms of availability of functions. However, there are still some major theoretical/computational problems with this approach, which includes the following:

1. We require a structurally stable cryptosystem, i.e. a system that has (almost) the same cycle length and Lyapunov exponent for all initial conditions. Most of the known pseudo-chaotic systems do not possess this property and there is no rigorous analytical method, as yet, for assessing this property.

2. There is still no theoretically plausible method for evaluating a chaotic system in terms of the necessary/sufficient conditions and properties that will absolutely guarantee the unpredictability of the system to acceptable cryptographic standards.

3. Deterministic chaotic algorithm have relatively low cycle lengths. Chaos based algorithms currently rely on the use of floating point arithmetic and require high precision FP arithmetic to generate reasonably large cycles Designing algorithms that output bit streams directly would therefore be a significant advantage.

4. There is currently no counterpart of a trapdoor transformation, as yet, known in chaos theory. Thus asymmetric chaos-based cryptographic protocols are not yet in sight.

In all literature on chaotic Cryptosystems, two categories were considered:
1. Synchronization Based Cryptosystems (Continuous): This was first developed by L.M. Pecora and T.L Carroll (Pecora and Carroll, 1990). This category can either be implemented on a digital or analog devices. This are based on synchronizing two or more continuous systems.
2. Non-Synchronization Based Cryptosystems (Digital): These cryptosystems includes Baptista cryptosystem (Baptista, 1998) and the Alvarez cryptosystem (Alvarez et al., 1999b). These are chaos bases systems that are based on digital chaos. They are realized in a finite environment. A digital chaos based cryptosystem can be implemented either by a stream cipher or a block cipher. This thesis focuses on the generation of pseudorandom sequences with a view to be implemented as running keys in stream ciphers. Chaotic systems

are used in digital chaotic ciphers to generate pseudorandom key-stream to be used as keys during encryption and decryption.

Chaos is exhibited in a portion of deterministic nonlinear systems. For a continuous system it is required that the system be of dimension three and above, while for discrete systems a one dimensional system could exhibit chaotic phenomena. There is a set of properties that summarize the characteristics observed in chaotic systems. These are considered the mathematical criteria that define chaos. The most relevant are the main characteristics of a chaotic system which relates directly to what makes a cryptographic system good or secure (confusion and diffusion).

Table 1.2: Similarities between Chaos and Cryptography

Chaos Based Cryptosystem	**Traditional Cryptosystem**
Floating point arithmetic	Integer arithmetic
Slow computation	Fast computation
Based on any nonlinear function	Usually based on the mod function
Does not necessitate prime numbers	Usually based on prime numbers
Low cycle length	High cycle length
Statistical bias	No statistical bias
Data superfluous	Data companionable
Chaos Theory	**Cryptography**
Chaos based system	Pseudo-chaos based system
Indiscriminate transformation	Indiscriminate transformation
Infinite number of stages	Finite number of stages
Infinite number of repetitions	Finite number of repetitions
Initial stage Plain text	Final stage Cipher text
Initial state and/or parameters	Keys
sensitive dependence	Confusion

1.4.1 Limitations of Chaos Based Cryptography

For many publications on chaos-based cryptosystems, only basic concepts are described whereas detailed implementation issues are neglected. However, generally speaking, implementation details are very important for cryptanalysts to evaluate the security of a cryptosystem. Also, the encryption speed and the implementation cost depend on such details. Therefore, the lack of implementation details generally makes it difficult to estimate the reliability and significance of the proposed cryptosystem through security analysis and performance evaluation. Thus, digital chaotic ciphers proposed in the literature had been confronted with a lot of security issues, with most of them not been able to pass security tests. To design a digital chaotic cipher that can be deemed to be a good one, a number of issues will have to be carefully considered. The following are the issues among others:

• **Quantization:**
Quantization is a process to convert a number into its representational value within a finite set of permissible values. Due to finiteness of the permissible set, quantization errors occurs in most implementations. These errors have been on study since the seminal work of Shannon and other researchers. A comprehensive study about quantization can be found in the work of M. R. Gray and D.L. Neuhoff (Gray and Neuhoff, 1998). The effect of quantization on chaos dynamics have been carried out. Earlier assumptions have it that chaotic systems are implemented with infinite precision. A great impact on the characteristics of a chaotic system when quantization process is undergone has been detected. For piecewise linear maps, cycle length, non-ideal distribution and correlation functions, have been reported by Li et al. (Li et al., 2001b). In finite machines, numbers are represented in binary form. Let ϵ be the distance between two neighboring points in the set of representable within a particular precision. Due to the binary representation, ϵ is always a power of 2. The index could either be positive, negative or zero depending on the finite arithmetic considered. When the phase space is subjected to integer discretization $\epsilon = 2^n$ where $n \geq 0$ is fixed for the throughout the space. When the reals in the space are discretized with a fixed point representation, $\epsilon = 2^{-n}$ where $n > 0$ is fixed for the whole space. $\epsilon = 2^{n(x)}$ for a floating point discretization of the reals in the phase space where $n(x) > 0$ depends on the precision of $\tilde{x}$, the discretized version of x.

Assuming that n-bit representation is adopted that is $\tilde{x} = 0.b_1 b_2 \dots b_n$, and according to different approximation functions, two of which are considered here (rounding and truncation) discretized form of the considered maps can be expressed as follows:

Logistic Map:

$$\begin{aligned} x_{i+1} &= \lambda\left(\frac{\tilde{x}_i}{2^n - 1}\right)\left(1 - \frac{\tilde{x}_i}{2^n - 1}\right) \\ \tilde{x}_{i+1} &= Q\Big((2^n - 1)x_{i+1}\Big) \end{aligned} \tag{1.38}$$

Skew-Tent Map:

$$\tilde{x}_{i+1} = \begin{cases} Q\left(\frac{\tilde{x}_i}{\tilde{\alpha}}\right), & \text{if } 0 \leq \frac{\tilde{x}_i}{2^n - 1} \leq \tilde{\alpha} \\ Q\left(\frac{2^n - \tilde{x}_i - 1}{1 - \tilde{\alpha}}\right), & otherwise \end{cases} \tag{1.39}$$

where $\tilde{\alpha} = \frac{k}{2^n - 1}$ and $k \in \{1, 2, \dots, 2^n - 2\}$.

Chebyshev Map:

$$\begin{aligned} x_{i+1} &= cos\left(4cos^{-1}\left(\frac{2\tilde{x}_i+1}{2^n-1}\right)\right) \\ \tilde{x}_{i+1} &= Q\left(\frac{(2^n-1)x_{i+1}-1}{2}\right) \end{aligned} \tag{1.40}$$

Sawtooth Map:

$$\begin{aligned} x_{i+1} &= a\left(\frac{\tilde{x}_i}{2^n}m\right) mod 1 \\ \tilde{x}_{i+1} &= Q((2^n)x_{i+1}) \end{aligned} \tag{1.41}$$

where $a > 0$. For all maps above, $g(\cdot)$ is an approximation function.
This concludes that quantization will have an adverse effect on the chaotic dynamics, where short periodic cycles and fixed point problem are observed. This effect will also greatly affect the performance of a random number generator based on the maps considered.
Extensive simulation has been conducted on the quantized version of these maps in our paper (Said et al., 2017), it can be concluded that short cycle length problem exists in most of the chaotic maps, such as logistic map, Chebyshev map, skewed tent map and sawtooth map. The obtained cycle length of discretized Chebyshev map or logistic map is much less than 2^n for almost all the cases. A relatively better result is observed for skewed tent map and sawtooth map, while the cycle length is higher than 2^n for some cases. For skewed tent map, the cycle length may even close to the maximum possible cycle length 2^n. Another problem after quantization is the existence of fixed-points. By estimating the accumulated percentage of the initial values that map to a fixed point, it is noticed that the discretized Chebyshev map and logistic map are poor performers. A large percentage value will eventually fall to a fixed point, and there exists an obvious increasing trend for both cases. For discretized skewed tent map using ceiling and flooring function, or the discretized sawtooth map with particular value of a, the accumulated percentage remains as a constant in a low level.

• **Encryption Speed:**
While the chaotic systems are running in finite precision, the floating-point or fixed-point arithmetic must be utilized. The floating-point arithmetic has been reported to be much slower than the fixed-point arithmetic. During real-time encryption, speed is a desired requirement. Some digital chaotic ciphers work so slowly that they are infeasible for real-time encryption (Baptista, 1998; Kotulski et al., 1999; Li et al., 2001b). The choice of finite arithmetic must be made, from either floating-point or fixed-point arithmetic. Since the floating-point arithmetic is much slower than the fixed-point (Li et al., 2001b), we will advice the use of fixed-point arithmetic. The piecewise linear chaotic maps are have considerable speed during implementation, as only one division and several additions are needed in an iteration. The use of multiple

chaotic iterations to generate one ciphertext has been found to lower the encryption speed (Li et al., 2001b). Throughout this thesis the used of fixed point arithmetic is assumed unless otherwise stated.

• **Practical Security:**
The claim of security of chaos based cryptosystems cannot be substantiated due to lack of a clearly defined procedure. The deterministic nature of discrete chaos, has made it possible to be put under some level of control. With this control, some information about the chaotic systems can be derived from their orbits. Such information can be catastrophic as it can be used to lessen the complexity of determining the key when such a system is used for its (key) generation. A number of authors of digital chaotic ciphers claimed them to be secure, but many are actually not, because of the deterministic nature of chaotic systems, there are some tools used in chaos theory to discern chaos. An adversary is likely to find some information about the chaotic systems from their orbits, which he might use to lessen the complexity of finding the secure key. For almost all digital chaotic ciphers the ciphertext directly depends on the chaotic orbit of a single chaotic system (Alvarez et al., 2000; Tao et al., 1998; Hong and Xieting, 1997; Zhou et al., 1997), so the extraction of such information may be possible. The cryptanalysis of a chaotic cryptosystem whose keystream depends on multiple chaotic orbits is more difficult since the output is determined by many different mixed chaotic orbits.

1.4.2 Finite Implementation of Chaotic Maps

Any designed cryptosystem can either be implemented in a software or a hardware, during which the cost of implementation is observed. Due to the high cost of floating-point arithmetic, the fixed point is preferred. Another desired requirement is the extensible security with considerably more cost and complexity. In fact, problems of realization are the crucial factors influencing the use of a cipher in many final applications, since there are so many kinds of ciphers that can provide enough security. Hardware and software realization at low cost is a very important requirement for a good digital cipher. Thus, the fixed-point arithmetic is better choice than floating-point which is more expensive to implement. Extensible security with considerably more cost and complexity is another desired requirement. In fact, problems of realization are the crucial factors influencing the use of a cipher in many final applications, since there are so many kinds of ciphers that can provide enough security. Although many of the problems have not been resolved in most digital chaotic ciphers, we still believe that chaotic and conventional cryptology will benefit each other from the mutual relationship/similarities existing between them.
Within the last decade, sequences derived from chaotic phenomena are being considered for use in secure communication, spread spectrum systems and cryptography. Chaotic sequences are generated from nonlinear dynamic systems. These are unpredictable, deterministic systems, often described by the system of parametrized differential equations (continuous time, eg. Lorentz system, Chua's oscillator, etc) or difference equations (discrete time eg Logis-

tic, tent, Bernoulli etc). Their essential feature is that they exhibit noisy-like behavior because of its strong sensitivity to initial conditions.
These are sequences generated iteratively from maps of the form $x_{k+1} = f(x_k)$ where $k = 0, 1, 2, \dots$ with x_0 being the initial state. The function f is mostly nonlinear, thus, a chaotic map can be regarded as a first order non-linear, time discrete, dynamical equation used iteratively to generate chaotic sequence $(x_0, x_1, x_2, \dots)$.
Determinism, nonlinearity, aperiodicity, non-converging and boundedness are properties characterized with chaos (Alligood et al., 2008), the main of which is sensitivity to initial conditions. Amplitude of iterates are generally bounded within the intervals $[0, 1]$, $[-1, 1]$ or $[-0.5, 0.5]$. One of the many qualities that made chaotic sequences appealing for cryptography is its very low cross correlation properties. Due to sensitive dependence on initial conditions, with small perturbation of an initial condition, the two chaotic sequences separate rapidly from each other after a short time period and are highly uncorrelated. Therefore, by using different initial values, it is possible to produce a large number of chaotic sequences which are pairwise highly uncorrelated.

1.5 Binary Sequences

With the advent of secure communication, the spread spectrum (SS) sequences were used by the military for secret communications. Spread spectrum is a means of transmission in which the signal takes in excess of the minimum bandwidth necessary to send the information. The band-spread is accomplished by means of a code sequence which is independent of the data and a synchronized reception with the code sequence at the receiver is used for de-spreading and subsequent data recovery. SS based communication systems are characterized with low probability of interception (LPI), immunity against jamming and separation of multi-path signals. Direct sequence spread spectrum (DSSS), in which the information signal is first modulated and then spread in bandwidth prior to transmission over the channel, is the most widely used technique of the SS. The sequences used for spreading is a noise like wide band sequence having good autocorrelation property. The periodic autocorrelation function is nearly two valued with peaks at zero shift and zero elsewhere.

Ideally, one would prefer a random binary sequence as the spreading sequence. However, practical synchronization requirements in the receiver, necessitates one to use Pseudorandom binary sequences. Such sequences (inherently periodic) that have been widely accepted for cryptographic usage includes: m-sequences, Gold codes, Kasami sequences, Quaternary sequences, Walsh functions etc.
One of the most commonly used sequences in spread spectrum (SS) communication is what is referred to an m-sequence (Golomb et al., 1967) generated using a linear feedback shift register (LFSR). Other sequences in use include the Gold and Kasami sequences, these sequences are mostly used with Direct Sequence Code Division Multiple Access (DS-CDMA). Gold sequences are generated by bit-by-bit modulo-2 addition of the two maximum length

sequences generated by using two distinct LFSR of same number of stages. A procedure similar to that used for generating Gold sequences can generate Kasami sequences.
The cross correlation of the spreading sequences are expected to be bounded, which can be measured using either the Welch bound (Welch, 1974) and/or the Sidelnikov bound (Sidelnikov, 1971). These two bounds were found to be satisfied by the Siddiqi-Udaya sequences (Tang et al., 2007).

The quality of a binary communication system depends on the ability of the receiver to detect the correct binary string sent. If a message is sent with a considerably long sequence, the average number of detected binary bits in error at the receiver end is called the bit error rate (BER). BER is an important tool in binary communication systems. In a DS-CDMA system the average BER performance depends on the bit energy, white noise power spectral density (PSD), number of simultaneous users and the normalized mean square value of cross correlation of the spreading sequences assigned to the users.

The linear complexity of SS sequences is another important parameter that needs to be determined. Linear complexity (LC) of a periodic sequence is the length of the shortest linear feedback shift register that can be used to generate the sequence (Massey J.L. 1969). Spreading sequences having larger linear complexity are considered to be good. The necessary security to the CDMA systems can be achieved by having sequences with large linear complexity, which will require a cryptanalyst to have knowledge of a large segment of the code sequence in order to be able to recover the complete code sequence.

Random number generation is one of the important technologies for several engineering applications such as Monte Carlo simulations, cryptosystems, spread spectrum CDMA communications. One of methods to generate aperiodic sequences is to use chaos which is defined as random phenomena generated by simple deterministic systems. There have been many research works on random number generation based on chaos (Bernstein and Lieberman, 1990; Kohda and Tsuneda, 1997; Argyris et al., 2010; Barakat et al., 2013; Cicek et al., 2014).

Cryptography requires the use of Random binary bits in a wide variety of situations. The inability to control the physical process that generates True Random Numbers (TRN) limits its use as a source of random bits to be used in cryptographic applications. Alternatively, a Pseudorandom Number Generator (PRNG) can be used in place of a TRNG. PRNG takes a small bit length seed (random) as input and produces a very large binary sequence which appears to be random. The concept of PRNG motivates the design of stream ciphers. From the word 'pseudo', pseudorandom numbers are actually not random, but assumes the properties of random numbers. PRNGs are algorithms that use mathematical formula to produce sequence of numbers that appear random.

PRNGs are efficient, in the sense that they are fast in production and deterministic. Efficiency is a required characteristic if your application needs large numbers, and determinism is handy if you need to replay the same sequence of numbers again at a later stage as is obtained in cryptography. PRNGs are typically periodic, which means that the sequence will eventually repeat itself due to finite precision. While periodicity is hardly ever a desirable characteristic, modern PRNGs have a period that is so long that it can be ignored for most practical purposes. This long periods are sufficient for the minimum length required by the cryptosystem.

1.5.1 Pseudorandom Number Generators

The difficulties of obtaining uniform random sequences from TRNG has made many researchers focused on the development of PRNGs. This becomes more appealing especially after the launch of digital computers. Due to their (pseudorandom numbers) portability and reproducible (lacking in TRNs), a wide range of applications have been explored. Simply put, a pseudorandom number generator is a finite state machine whose output sequences are indistinguishable from those of a truly random number generator by any polynomial-time test algorithm.

These are Sequences, which are generated by deterministic algorithms so as to simulate truly random sequences. A pseudorandom sequence in the unit interval $[0, 1]$ is called a sequence of pseudorandom numbers (PRNs). In particular, for a prime p, the elements $\{0, 1, 2, \ldots, p-1\}$ of the finite field $\mathbb{F}_p$ generates the sequence. We present here some few examples of PRNGs:

• **Linear congruential generators:**
The linear congruential generator (LCG) is defined by the relation:

$$f(X) = aX + c \; mod \; m \tag{1.42}$$

where a and c are constants and $X \in \{0, 1, 2, \ldots m-1\}$ The quality of this generator depends on the choice of the constants a and c, thus they should be chosen carefully. Due to the strong correlation between X_n and X_{n+1}, the LCG has poor quality and hence not a good generator.

• **Multiple-recursive generators:**
This generator is simply defined by:

$$X_n = (a_1 X_{n-1} + a_2 X_{n-2} + \cdots + kX_{n-k}) mod \; m \tag{1.43}$$

with its state space as $\{0, 1, 2, \ldots, m-1\}^k$. At the time instant t, the state of the generator is $x_t, x_{t-1}, \ldots, x_{t-k+1}$. The maximum period of $m^k - 1$ could be realized with a suitable choice of a_i and m.

• **Blum Blum Shub (BBS) Generator:**

Named after its inventors, Lenore Blum, Manuel Blum and Michael Shub, the BBS generator is give by:

$$X_j = X_{j-1} mod\ N \tag{1.44}$$

where the seed is $X_0 = X^2 mod\ N$ and $N = Q_1 Q_2$ is the product of two large primes such that $Q_i \equiv 3 mod\ 4$ and S is a random number such that gcd(S,N) =1 (Blum et al., 1983).

• **Combining generators:**
This entails a combination of a number of random number generators. For a given combination of n generators we will have

$$\begin{aligned} X_i^{(1)} &= a_1 X_{i-1}^{(1)}\ mod\ m_1 \\ X_i^{(2)} &= a_2 X_{i-1}^{(2)}\ mod\ m_2 \\ &\vdots \\ X_i^{(n)} &= a_n X_{i-1}^{(n)}\ mod\ m_1 \end{aligned} \tag{1.45}$$

with its corresponding state space given by $\{0, 1, 2, \ldots, m_1 - 1\} \times \{0, 1, 2, \ldots, m_2 - 1\} \times \cdots \times \{0, 1, 2, \ldots, m_n - 1\}$. An example is the Wichman-Hill generator which combines three linear congruential generators. These generators have been in the forefront in the generation of pseudorandom binary sequences used in classical cryptography.

1.5.2 Chaotic Binary Sequences

These are sequences generated from chaotic maps. They come from the trajectories of the map discretized in the field required. Since we are interested in generating binary sequences, the discretization will be within the field $\mathbb{F}_2$. With cryptographic applications, generating pseudorandom sequences through linear methods (like the LFSR and the LGC) are highly not recommended. This is due to the fact that there exist efficient algorithms that predicts such sequences due to there short cycles. This is a very serious weakness in the realm of cryptography. According to Kwok et. al. (Kwok and Tang, 2007), linear methods generate numbers lying on regular lattices, where turples of generated sequences form vectors that belongs to a lattice structure. Thus therefore, linear recurrences are not suitable for qualitative sequences for cryptographic applications (Menezes et al., 1996). Thus the need for generating sequences using nonlinear based algorithms is required. Chaotic systems, due to their non-linearities, can be used in defining nonlinear generators with both efficient implementation and good statistical properties.

A chaotic random bit generator (CRBG) carries some features of true and pseudo RBGs since chaotic systems yield aperiodic signals, but produced from deterministic systems. Thus, the chaotic systems can be a good source for ran-

dom bit generators and related applications of both cryptography and simulation. A wide range of discrete time and continuous time chaotic systems may be used as random number sources. As a measure of the randomness, the positive Lyapunov exponents of the chaotic systems determine the entropy of the signals. However, the positive Lyapunov exponent does not provide any information about unbiased or uncorrelated features of random numbers. Hence, for extracting unbiased and uncorrelated random bits from chaotic sources, a post-processing is needed.

A random bit generator (RBG) often consists of three stages as demonstrated in Figure 1.13. The first and main stage is the random number (binary) source. This stage generates then stream of random numbers. The second stage is that which post-processes the generated random numbers. The binary generator and post-processor stages also have important roles for extracting statistically independent and efficient random bits. The random number sources can be random (true) or pseudorandom sources depending on the application. The true random number sources are hardware-based, non-deterministic, aperiodic and taking considerably long time to produce numbers. The pseudorandom numbers are software based, deterministic, periodic, efficient and suitable for specifically simulation modeling and cryptography.

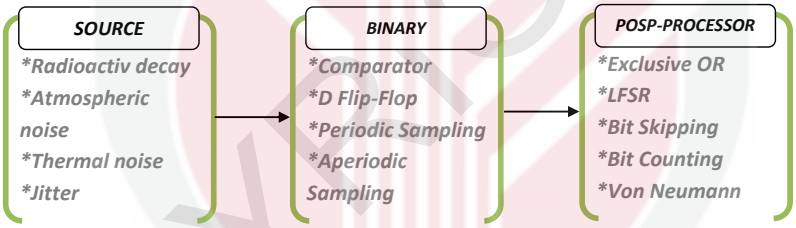


Figure 1.13: Steps for Random bit generation

1.5.3 LFSR Sequences

Linear Feedback Shift Registers (LFSRs) were introduced into stream cipher application as early as the year 1950. These linear recurring registers are easy to implement by hardware and fast to process, LFSRs were often recommended to be the pseudorandom sequences generators. The use of LFSRs in stream ciphers has given cryptographers and mathematicians the opportunity to use rigorous mathematical theory to analyze their security. Due to their generation by linear devices, their linear complexity is a vital concept to determine the security levels of stream ciphers on which they are used. Complexity measurements such as higher-order complexity, 2-adic complexity measures and complexity measures based on pattern counting are used. Another important measure of complexity, the linear complexity profile is also a good tool to measure the randomness of generated sequences. The areas of

synchronization, masking, scrambling of codes, white noise, and signal sets in CDMA communications, has been largely dependent on the use of Feedback Shift Register (FSR) sequences. FSR sequences have equally gained prominence in main stream cryptographic applications, areas like stream cipher key stream generation, random number generation.
Let $B^n = \{0,1\}^n$ be an n-dimensional vector space given by:

$$B^n = \{(s_0, s_1, s_2, \ldots, s_{n-1}) | s_i \in \{0,1\}\}. \tag{1.46}$$

The function f, called the feedback function, is defined by the mapping $f : B^n \to \{0,1\}$ such that:
$f(s_0, s_1, s_2, \ldots, s_{n-1}) = \sum_{i=0}^{n-1} a_i s_i$ and $s_{n+k} = f(s_k, s_{k+1}, s_{k+2}, \ldots, s_{k+n-1})$, $k = 1, 2, \ldots$. The initial state is $(s_0, s_1, s_2, \ldots, s_{n-1})$ and $(a_1, a_2, a_3, \ldots, a_\ell)$ are coefficients in the feedback function f. The word linear is derived from nature of the function f, of being linear. When f is a nonlinear function, then we have a Nonlinear Feedback Shift Register (NLFSR).

Definition 1.10 *A binary LFSR is an electronic device with N memory elements (stages), cyclic shifting and linear feedback. Binary sequences drawn from the alphabet* $\{0,1\}$ *are shifted through the shift register after each time interval, the register shifts all its contents to the right. The particular 1's and 0's occupying the shift register stages after a time instant are called states.*

A linear feedback shift register of length ℓ, with coefficients $a_1, a_2, a_3, \ldots, a_\ell \in \mathbb{F}_2$, with initial state $s_0, s_1, s_2, \ldots, s_{\ell-1} \in \mathbb{F}_2^\ell$ whose state update function f is given by:

$$(s_0, s_1, s_2, \ldots, s_{k-1}) \Rightarrow \left(s_0, s_1, s_2, \ldots, s_{\ell-1}, \sum_{i=0}^{\ell} a_i s_{\ell-i}\right) \tag{1.47}$$

The output sequence $a = s_0, s_1, s_3, \ldots$, of an LFSR of length ℓ satisfies a linearly recurrence relation for all $(n \geq \ell)$. The shift register is controlled by an external clock, at a given time unit t, each digit is shifted one stage to the right. The content of the rightmost stage s_t is output. The new content of the leftmost stage is the feedback bit $s_{t+\ell}$ as illustrated in Figure 1.14.

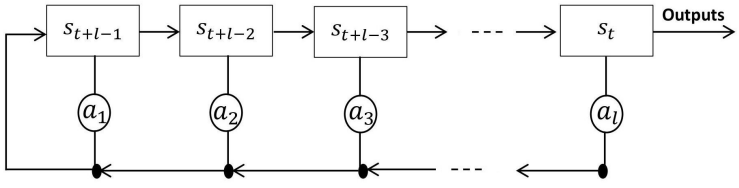


Figure 1.14: Linear feedback shift register of length ℓ.

The output sequence of an LFSR is uniquely determined by its feedback coefficients and its initial state. The feedback coefficients $a_1, a_2, \ldots, a_\ell$ of an

LFSR of length ℓ are usually represented by the LFSR feedback polynomial (or connection polynomial) defined by

$$F(X) = 1 - \sum_{i=1}^{\ell} a_i X^i \tag{1.48}$$

or in terms of its characteristic polynomial:

$$F^*(X) = X^\ell F(1/X) = X^\ell - \sum_{i=1}^{\ell} a_i X^{\ell-i}. \tag{1.49}$$

A maximum-length LFSRs is one whose output sequences have maximum period of length $2^\ell - 1$. It cycles through $2^\ell - 1$ different states excluding the zero state.

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 s_{n-3} + \cdots + a_\ell s_{n-\ell} \tag{1.50}$$

where the a_{is} are called the coefficients of the recurrence relation. Equation (1.50) can be expressed in polynomial form as:

$$a(x) = -1 + \sum_{i=1}^{\ell} a_i x^i \in \mathbb{F}_2[x] \tag{1.51}$$

with $a_i \in \mathbb{F}_2$, equation (1.51) is called the feedback polynomial. It is inverse to the characteristic polynomial of the above linear recurrence relation.

1.5.4 Algebraic Description of LFSR Sequences

We especially want to find a closed formula for an LFSR sequence. One way to achieve this is to study the companion matrix of the LFSR sequence. With an apriori knowledge that convolutional codes (in coding theory) will be used, we here present an alternative definition of the LFSR sequence called the linear matrix method. Given the sequence $s_n = a_1 s_{n-1} + a_2 s_{n-2} + \ldots a_\ell s_{n-\ell}$, it can be represented in the following matrix form:

$$\begin{bmatrix} \mathrm{s}_n \\ \mathrm{s}_{n-1} \\ \vdots \\ \mathrm{s}_{n-\ell+1} \end{bmatrix} = \begin{bmatrix} \mathrm{a}_1 & \ldots & \mathrm{a}_{\ell-1} & \mathrm{a}_\ell \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{bmatrix} \begin{bmatrix} \mathrm{s}_{n-1} \\ \mathrm{s}_{n-2} \\ \vdots \\ \mathrm{s}_{n-\ell} \end{bmatrix}$$

which is expressed in the equation (1.53) by the use of its corresponding companion matrix:

$$(s_n, s_{n-1}, \ldots, s_{n-\ell+1}) = [s_{n-1}, s_{n-2}, \ldots, s_{n-\ell}] \begin{bmatrix} a_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & 0 & \ldots & 1 \\ a_n & 0 & \ldots & 0 \end{bmatrix} \quad (1.53)$$

and thus iteration is performed by:

$$\begin{bmatrix} s_{n-1} \\ s_{n-2} \\ \vdots \\ s_{n-\ell} \end{bmatrix} = \begin{bmatrix} a_1 & \ldots & a_{\ell-1} & a_\ell \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{bmatrix}^{n-\ell} \begin{bmatrix} s_{\ell-1} \\ s_{\ell-2} \\ \vdots \\ s_0 \end{bmatrix}$$

with $(s_{\ell-1}, s_{\ell-2}, \ldots, s_0)$ as the initial state of the LFSR.

1.5.5 LFSR Sequences as Cyclic Linear Codes

The LFSR defines a linear mapping from its initial state $(s_0, s_1, \ldots, s_{n1})$ to its output sequence $(s_i)_{i\in\mathbb{N}}$. For fixed N we may interpret the mapping $C : (s_0, s_1, \ldots, s_{n1}) \mapsto (s_0, s_1, \ldots, s_{n1})$ as a linear code of length N and dimension n. A parity check matrix of the code is:

$$H = \begin{bmatrix} \mathrm{c}_0 & \ldots & \mathrm{c}_{n-1} & \text{-1} & 0 & \ldots & & 0 \\ 0 & \mathrm{c}_0 & \ldots & \mathrm{c}_{n-1} & \text{-1} & 0 & \ldots & 0 \\ \vdots & & \ddots & & \ddots & \vdots & \vdots & \\ 0 & & \ldots & 0 & \mathrm{c}_0 & \ldots & \mathrm{c}_{n-1} & \text{-1} \end{bmatrix}$$

If we consider the full period of the LFSR, then the resulting linear code is cyclic. The code C also has a unique systematic generator matrix:

$$G = \left[\begin{array}{ccc|ccc} 1 & & 0 & \mathrm{c}_{n,0} & \ldots & c_{N-1,0} \\ & \ddots & & \vdots & & \vdots \\ 0 & & 1 & \mathrm{c}_{n,n-1} & \ldots & c_{N-1,n-1} \end{array}\right]$$

We have $(s_0, s_1, \ldots, s_{N1}) = (s_0, s_1, \ldots, s_{n1})G$, i.e.

$$s_k = \sum_{i=0}^{n-1} c_{k,i} s_i \quad (1.56)$$

We will use the linear representation in equation (1.56) of the element s_k in terms of the initial state in an attack to be discussed later.

The maximum length sequences, mostly referred to as m-sequences are generated and characterized by a generator polynomial whose Properties can be derived using algebraic coding theory. They are the most popular spreading sequences realized, in the most simplest way, with LFSRs.

Does the LFSR sequence, as an encryption method, meet the four security objectives (Secrecy, integrity, non-repudiation and authentication)? The answer is no. With the secrecy objective: One cannot rely on LSFR sequences for secrecy because the minimal connection polynomial (which is the key necessary to generate the LFSR sequence used as the stream cipher) of the sequence is easily determined using the Berlekamp-Massey Algorithm. LFSR sequences on its own, provides very little integrity. If combined with some error-correcting codes however, one can realize a limited amount of integrity. Likewise, on its own, a LFSR sequence provides very little in terms of non-repudiation. When two separate LFSRs are considered between two parties and the credentials exchanged, authentication can be achieved.
Thus therefore, the use of binary sequences generated by LFSRs cannot be used for cryptographic purposes because three of the for security objectives of cryptography cannot be achieved.

1.6 Problem Statement

Random number generators, RNGs, are a fundamental tool in the areas of stochastic simulation and cryptography. In cryptography, these generators are employed to produce secret keys, encrypt messages or to mask the content of certain protocols and recently, in the area of internet gambling. As important as implementation of cryptographic protocols and algorithms is, a fundamental part of the entire process is the key generation. The second Kerckhoff's Principle states that the security of a cryptosystem shall not be based on secrecy of the algorithm but solely on the secret keys.

The output of any encryption/decryption algorithm, requires the use of a pseudorandom number generator (PRNG) to generate the keys. These PRNGs are designed such that secret state compromise does not occur due to poor design, error in implementation or choice of low quality seed. There are many standards that describe requirements, which should be fulfilled by PRNGs. Researchers are therefore faced with the challenge of generating sequences that meets the requirements of cryptography. Thus, generating sequences that meets these standards has remained a problem to be solved.

1.7 Research Questions

Has the existing methods of using linear functions/systems yielded the generation of sequences that meets the requirements of the cryptographic world? One of the most widely used methods of generating sequences has been the LFSR. This approach, despite its ease of implementation, has been criticized

because of linearity in the generation process. Most if not all sequences generated by LFSRs has been compromised by the ability of the recovery of the initial state of the LFSR using the Berlekamp Massey algorithm. Although LFSR sequences have many desirable properties, using the LFSR output sequence directly as keystream is not advisable due to the linearity of LFSR sequences. To make use of the desirable properties of the LFSR in a keystream generator for a stream cipher, it is necessary to introduce nonlinearity. To what extend will chaotic dynamics be used in improving the limitations of the linear-based generation procedures, which includes all methods (algorithms) based on LFSRs. Will the combination of chaos theory and linear functions produce a sequence that will meet the requirements of cryptography in terms of security?

1.8 Aims and Objectives

The main objective of this thesis is to determine the possibility of the use of one dimensional chaotic maps in the generation of pseudorandom binary sequences with a view to be implemented in cryptographic applications. Most binary sequences used as keys in cryptographic applications are generated by systems whose operations are linear. Since nonlinear sequences are considered more secure than linear sequences, non-linearity can be introduced in the generation of these sequences through either the update function(s), output function(s) or the combination of both. To achieve this, the thesis is partitioned into the following objectives:

- To determine the best binary generation function from the trajectories of the chosen one dimensional chaotic maps implemented in this thesis. It has been established already in the literature that one dimensional chaotic maps with equidistributivity property can be used to generate binary sequences with good statistical properties.
- To investigate the best possible algebraic presentation of the maps. We have shown that different representation of the same maps can generate different trajectories with the same initial conditions and computation precision. The determination of the minimum precision for a sequence that will satisfy the required statistical qualities and the distribution of bit patterns in the generated sequence.
- Best possible processing function to remove bias was to be determined. The usual linear post/pre-processing functions had been reported to have deficiencies, thus a nonlinear combiner generator will be designed to eliminate any bias that might have been embedded in the sequence generation process.
- To determine the statistics of the processed sequence, and the presence of state convergence in the sequence generated. This convergence may be exploited in a key-recovery-attack.

The use of pseudorandom sequences in the field of cryptography cannot be over emphasized. The proposals to generate these pseudorandom sequences has been presented in the literature, most of which are found to be far from the desired randomness required. This research aims to determine the quality of binary sequences generated from one dimensional chaotic maps for the purpose of cryptographic applications.

1.9 Scope of study

The use of chaotic systems in the generation of binary sequences has been a subject of research for some time now. These generation could either be based on continuous or discrete domain. In the continuous domain, a chaotic system of at-least three dimension is required to achieve chaos. With discrete maps, one dimensional maps achieve chaos with limited implementation complexity as against higher dimensions. The study is limited to the pseudorandom sequence generation from a class of one dimensional chaotic maps with equidistributivity and constant summation properties. These maps are used to generate binary sequences whose statistical properties were determined. The defects associated with chaos based binary sequences were improved to meet serious cryptographic applications by processing using nonlinear combiner generator. These generator serves as a processing mechanism to improve the statistical requirements of the directly derived chaos based binary sequences. The non-linearity of the sequences resulting from the combiner generator is injected into the chaos based sequences thereby enhancing its qualities. The research is limited to harnessing the good qualities of LFSRs and chaos theory (in form of 1D chaotic maps with equidistributivity and constant summation property) towards generating a sequence that meets statistical requirements of cryptography. One dimensional maps generates identically distributed binary sequences and they have been used as deterministic generators of unpredictable sequences. If chaos can be realized with 1D maps which has very little complexity of implementation, one needs not engage higher dimensional maps whose complexity of implementation is much higher. All the considered 1D maps have a well defined probability distribution functions.

1.10 Significance of Study

The security paradigm in modern cryptology has been shifted from ciphers to keys (Kerckhoffs's principle), since many ciphers are broken as a result of progressive developments in computer science. In modern cryptology, secrecy is based on keys which are basically random numbers. A cryptosystem is only as secure as its RNG generating the keys. A failure in the pseudorandom sequence generation mechanism can surely be catastrophic to the entire cryptosystem, exposing the overall cryptosystem to cryptanalysis.
The generation of pseudorandom numbers in cryptography is near to the most important aspect of the science of cryptology. The use of such numbers in the generation of keys used in encryption and decryption has remained vital. By

the Kirchhoff's principle, the security of any cryptosystem is expected to depend only on the keys while all components of the system are expected to be public. The quality of these sequences depends on their statistical properties, which largely depends on the generation mechanism. Determining these statistical properties, and fulfilling the minimum requirement for cryptographic application has always been a subject for continuous research.

1.11 Organization of the Thesis

Chapter one gives the basic introduction to the idea of dynamical systems, chaos and cryptography. Dynamical systems, both continuous and discrete were introduced with more emphasis on the discrete aspect since its the bedrock of this research. The class of 1D maps with equidistributivity property were introduced. A number of 1D chaotic maps has been considered, their precision arithmetic and quantization were elucidated. The notion of binary sequences was discussed with consideration on chaos based and LFSR based sequences.

Chapter two is a literature review of the related works undertaken in the area of interest to this research. The review was presented along the headings of the main topics of the thesis: Pseudorandom Number Generation, Chaos Based Pseudorandom Sequences, Processing Chaos Based Sequences.

Chapter three is concerned with the aspect of discrete dynamics of chaotic maps, resulting in the extraction of binary sequence from the trajectory of the maps. The realization of these trajectories with respect to finite precision arithmetics is discussed. Numerical computation of the trajectories of such maps based on fixed and floating point arithmetic are discussed. Various algebraic representation of Logistic map as an example of the kinds of maps considered is presented. The statistical qualities of sequences generated from these different kinds of representations were determined. The methods of generating chaos based pseudorandom bits is discussed. The statistics of each of the methods has been considered with a view to identify the best approach to be adopted during sequence generation. The extracted bits were subjected to post-processing techniques and their correlation analysis discussed.

Chapter four dwells of finding a way of realizing chaos based pseudorandom bits with the required statistical properties that will be suitable for cryptographic application. A pseudorandom generator is proposed, this generator uses a nonlinear combiner generator as part of the generation mechanism. This nonlinear combiner has been discussed, giving details of characteristics and cryptographic properties of the considered Boolean functions. The nonlinear combiner serves a clocking device that determines the iterations in the chaos based binary generation phase. It injects some required properties in the generation of chaos based binary sequences, which is long period and reduced correlation between successive bits in the sequence. These results in a sequence with good statistical properties.

Chapter five is on the analysis of the proposed generator in chapter four. The nonlinear combiner part of the generator is analyzed with correlation (fast) attack and correlation attack using convolutional codes, in order to determine the strength of the clocking sequence. The clocking sequence defines the order of combination of the chaotic trajectory of the two maps used in generating the chaos based sequences.

Finally chapter six is the summary of the main findings of the research and conclusions drawn regarding the significance of the reported results. Recommendations for further research has been suggested.

REFERENCES

Aboites, V., Liceaga, D., Kir'yanov, A., and Wilson, M. (2016). Ikeda map and phase conjugated ring resonator chaotic dynamics. *Appl. Math*, 10(6):1–6.

Addabbo, T., Alioto, M., Bernardi, S., Fort, A., Rocchi, S., and Vignoli, V. (2004). The digital tent map: performance analysis and optimized design as a source of pseudo-random bits. In *Instrumentation and Measurement Technology Conference, 2004. IMTC 04. Proceedings of the 21st IEEE*, volume 2, pages 1301–1304. IEEE.

Addabbo, T., Alioto, M., Fort, A., Rocchi, S., and Vignoli, V. (2005). Long period pseudo random bit generators derived from a discretized chaotic map. In *2005 IEEE International Symposium on Circuits and Systems*, pages 892–895. IEEE.

Addabbo, T., Alioto, M., Fort, A., Rocchi, S., and Vignoli, V. (2006a). The digital tent map: Performance analysis and optimized design as a low-complexity source of pseudorandom bits. *IEEE Transactions on Instrumentation and Measurement*, 55(5):1451–1458.

Addabbo, T., Alioto, M., Fort, A., Rocchi, S., and Vignoli, V. (2006b). A feedback strategy to improve the entropy of a chaos-based random bit generator. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 53(2):326–337.

Ahmed, E., El-Sayed, A., and El-Saka, H. A. (2006). On some routh–hurwitz conditions for fractional order differential equations and their applications in lorenz, rössler, chua and chen systems. *Physics Letters A*, 358(1):1–4.

Alligood, K. T., Sauer, T. D., Yorke, J. A., and Crawford, J. (2008). Chaos: An introduction to dynamical systems. *Physics Today*, 50(11):67–68.

Alvarez, E., Fernandez, A., Garcıa, P., Jiménez, J., and Marcano, A. (1999a). New approach to chaotic encryption. *Physics Letters A*, 263(4):373–375.

Alvarez, G., Montoya, F., Romera, M., and Pastor, G. (2000). Cryptanalysis of a chaotic encryption system. *Physics Letters A*, 276(1-4):191–196.

Alvarez, G., Montoya, F., Romera, M., and Pastor, G. (2003). Cryptanalysis of an ergodic chaotic cipher. *Physics Letters A*, 311(2-3):172–179.

Alvarez, G., Montoya, P., Pastor, G., and Romera, M. (1999b). Chaotic cryptosystems. In *Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on*, pages 332–338. IEEE.

Argyris, A., Deligiannidis, S., Pikasis, E., Bogris, A., and Syvridis, D. (2010). Implementation of 140 gb/s true random bit generator based on a chaotic photonic integrated circuit. *Optics express*, 18(18):18763–18768.

Bakiri, M., Guyeux, C., Couchot, J.-F., Marangio, L., and Galatolo, S. (2018). A hardware and secure pseudorandom generator for constrained devices. *IEEE Transactions on Industrial Informatics*, 14(8):3754–3765.

Baptista, M. (1998). Cryptography with chaos. *Physics Letters A*, 240(1):50–54.

Barakat, M. L., Mansingka, A. S., Radwan, A. G., and Salama, K. N. (2013). Generalized hardware post-processing technique for chaos-based pseudorandom number generators. *ETRI Journal*, 35(3):448–458.

Belkhouche, F., Qidwai, U., Gokcen, I., and Joachim, D. (2004). Binary image transformation using two-dimensional chaotic maps. In *Proceedings of the 17th International Conference on Pattern Recognition. ICPR 2004.*, volume 4, pages 823–826. IEEE.

Bernstein, G. M. and Lieberman, M. A. (1990). Secure random number generation using chaotic circuits. *IEEE Transactions on Circuits and Systems*, 37(9):1157–1164.

Bianco, M. E. and Reed, D. A. (1991). Encryption system based on chaos theory. US Patent 5,048,086.

Biham, E. (1991). Cryptanalysis of the chaotic-map cryptosystem suggested at eurocrypt'91. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 532–534. Springer.

Blackburn, S. R. (1999). The linear complexity of the self-shrinking generator. *IEEE Transactions on Information Theory*, 45(6):2073–2077.

Blackledge, J. (2011). Cryptology. *Fractals and Chaos, Woodhead Publishing*.

Blahut, R. E. (1983). *Theory and practice of error control codes*, volume 126. Reading, (Ma): Addison-Wesley.

Blum, L., Blum, M., and Shub, M. (1983). Comparison of two pseudo-random number generators. In *Advances in Cryptology*, pages 61–78. Springer.

Blum, L., Blum, M., and Shub, M. (1986). A simple unpredictable pseudo-random number generator. *SIAM Journal on computing*, 15(2):364–383.

Blum, M. and Micali, S. (1984). How to generate cryptographically strong sequences of pseudorandom bits. *SIAM journal on Computing*, 13(4):850–864.

Borcherds, P. and McCauley, G. (1993). The digital tent map and the trapezoidal map. *Chaos, Solitons & Fractals*, 3(4):451–466.

Boyarsky, A. and Scarowsky, M. (1979). On a class of transformations which have unique absolutely continuous invariant measures. *Transactions of the American Mathematical Society*, 255:243–262.

Cafagna, D. and Grassi, G. (2012). Observer-based projective synchronization of fractional systems via a scalar signal: application to hyperchaotic rössler systems. *Nonlinear Dynamics*, 68(1-2):117–128.

Candido, R., Soriano, D. C., Silva, M. T., and Eisencraft, M. (2015). Do chaos-based communication systems really transmit chaotic signals? *Signal Processing*, 108:412–420.

Canteaut, A. and Filiol, E. (2000). Ciphertext only reconstruction of stream ciphers based on combination generators. In *International Workshop on Fast Software Encryption*, pages 165–180. Springer.

Cao, Y. (2013). A new hybrid chaotic map and its application on image encryption and hiding. *Mathematical Problems in Engineering*, 2013.

Carlet, C., Guillot, P., and Mesnager, S. (2006). On immunity profile of boolean functions. In *International Conference on Sequences and Their Applications*, pages 364–375. Springer.

Celikovsky, S. and Zelinka, I. (2010). Chaos theory for evolutionary algorithms researchers. In *Evolutionary Algorithms and Chaotic Systems*, pages 89–143. Springer.

Chaitin, G. J. (1975). A theory of program size formally identical to information theory. *Journal of the ACM (JACM)*, 22(3):329–340.

Chen, G. and Yu, X. (1999). On time-delayed feedback control of chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 46(6):767–772.

Chen, H., Zhang, S., Xu, N., Song, M., Li, X., Li, R., Zeng, Y., Hong, J., and You, L. (2018). Binary and ternary true random number generators based on spin orbit torque. In *2018 IEEE International Electron Devices Meeting (IEDM)*, pages 36–50. IEEE.

Cicek, I., Pusane, A. E., and Dundar, G. (2014). A novel design method for discrete time chaos based true random number generators. *INTEGRATION, the VLSI journal*, 47(1):38–47.

Clark Jr, G. C. and Cain, J. B. (2013). *Error-correction coding for digital communications*. Springer Science & Business Media.

Corinto, F., Krulikovskyi, V., and Haliuk, S. D. (2016). Memristor-based chaotic circuit for pseudo-random sequence generators. In *2016 18th Mediterranean Electrotechnical Conference (MELECON)*, pages 1–3. IEEE.

Courtois, N. T. (2003). Fast algebraic attacks on stream ciphers with linear feedback. In *Annual International Cryptology Conference*, pages 176–194. Springer.

Dar, K., Bakhouya, M., Gaber, J., Wack, M., Lorenz, P., et al. (2010). Wireless communication technologies for its applications. *IEEE Communications Magazine*, 48(5):156–162.

de la Fraga, L. G., Torres-Pérez, E., Tlelo-Cuautle, E., and Mancillas-López, C. (2017). Hardware implementation of pseudo-random number generators based on chaotic maps. *Nonlinear Dynamics*, 90(3):1661–1670.

Devaney, R. (2008). *An introduction to chaotic dynamical systems*. Westview press.

Dichtl, M. (2007). Bad and good ways of post-processing biased physical random numbers. In *International Workshop on Fast Software Encryption*, pages 137–152. Springer.

Ding, M., Grebogi, C., Ott, E., Sauer, T., and Yorke, J. A. (1993). Estimating correlation dimension from a chaotic time series: when does plateau onset occur? *Physica D: Nonlinear Phenomena*, 69(3-4):404–424.

Dmitriev, D., Sokolovskiy, A., Gladyshev, A., Ratushniak, V., and Tyapkin, V. (2019). Pseudorandom sequence generator using cordic processor. In *2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, pages 477–480. IEEE.

Driebe, D. J. (2013). *Fully chaotic maps and broken time symmetry*, volume 4. Springer Science & Business Media.

Eichenauer, J. and Lehn, J. (1986). A non-linear congruential pseudo random number generator. *Statistische Hefte*, 27(1):315–326.

ElShaarawy, I. and Gomaa, W. (2014). Ideal quantification of chaos at finite resolution. In *International Conference on Computational Science and Its Applications*, pages 162–175. Springer.

Erdmann, D. and Murphy, S. (1992). Hénon stream cipher. *Electronics Letters*, 28(9):893–895.

Fan, C., Xie, Z., and Ding, Q. (2018). A novel algorithm to improve digital chaotic sequence complexity through ccemd and pe. *Entropy*, 20(4):295–309.

Fang, C. F., Rutenbar, R. A., and Chen, T. (2003). Fast, accurate static analysis for fixed-point finite-precision effects in dsp designs. In *Proceedings of the 2003 IEEE/ACM international conference on Computer-aided design*, page 275. IEEE Computer Society.

Ferrenberg, A. M., Landau, D., and Wong, Y. J. (1992). Monte carlo simulations: Hidden errors from "good"random number generators. *Physical Review Letters*, 69(23):3382.

Fotiades, N. A. and Boudourides, M. A. (2001). Topological conjugacies of piecewise monotone interval maps. *International Journal of Mathematics and Mathematical Sciences*, 25(2):119–127.

François, M., Defour, D., and Negre, C. (2014). A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic. *Informatica*, 38(3).

Garcia-Bosque, M., Pérez-Resa, A., Sánchez-Azqueta, C., Aldea, C., and Celma, S. (2018). Chaos-based bitwise dynamical pseudorandom number generator on fpga. *IEEE Transactions on Instrumentation and Measurement*, 68(1):291–293.

Gilmore, R. and Lefranc, M. (2012). *The Topology of Chaos: Alice in Stretch and Squeezeland*. John Wiley & Sons.

Goldberg, D. (1991). What every computer scientist should know about floating-point arithmetic. *ACM Computing Surveys (CSUR)*, 23(1):5–48.

Golomb, S. W. et al. (1967). *Shift register sequences*. Aegean Park Press.

Grassberger, P. and Procaccia, I. (2004). Measuring the strangeness of strange attractors. In *The Theory of Chaotic Attractors*, pages 170–189. Springer.

Gray, R. M. and Neuhoff, D. L. (1998). Quantization. *IEEE transactions on information theory*, 44(6):2325–2383.

Günther, C. G. (1987). Alternating step generators controlled by de bruijn sequences. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 5–14. Springer.

Guyeux, C., Wang, Q., and Bahi, J. M. (2010). A pseudo random numbers generator based on chaotic iterations: application to watermarking. In *International Conference on Web Information Systems and Mining*, pages 202–211. Springer.

Habutsu, T., Nishio, Y., Sasase, I., and Mori, S. (1990). A secret key cryptosystem using a chaotic map. *IEICE TRANSACTIONS (1976-1990)*, 73(7):1041–1044.

Habutsu, T., Nishio, Y., Sasase, I., and Mori, S. (1991). A secret key cryptosystem by iterating a chaotic map. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 127–140. Springer.

Hamza, R. (2017). A novel pseudo random sequence generator for image-cryptographic applications. *Journal of Information Security and Applications*, 35:119–127.

Heidari-Bateni, G. and McGillem, C. D. (1994). A chaotic direct-sequence spread-spectrum communication system. *Communications, IEEE Transactions on*, 42(234):1524–1527.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. In *The Theory of Chaotic Attractors*, pages 94–102. Springer.

Herlestam, T. (1985). On functions of linear shift register sequences. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 119–129. Springer.

Hong, Z. and Xieting, L. (1997). Generating chaotic secure sequences with desired statistical properties and high security. *International Journal of Bifurcation and Chaos*, 7(01):205–213.

Huang, F. and Guan, Z.-H. (2005). A modified method of a class of recently presented cryptosystems. *Chaos, Solitons & Fractals*, 23(5):1893–1899.

Huang, X. (2012). Image encryption algorithm using chaotic chebyshev generator. *Nonlinear Dynamics*, 67(4):2411–2417.

Huang, X., Liu, L., Li, X., Yu, M., and Wu, Z. (2019). A new pseudorandom bit generator based on mixing three-dimensional chen chaotic system with a chaotic tactics. *Complexity*, 2019:6567198(1)–6567198(9).

Ikeda, K. (1979). Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. *Optics communications*, 30(2):257–261.

Jakimoski, G., Kocarev, L., et al. (2001). Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 48(2):163–169.

Jia, X. (2010). Image encryption using the ikeda map. In *Intelligent Computing and Cognitive Informatics (ICICCI), 2010 International Conference on*, pages 455–458. IEEE.

Jiang, H., Belkin, D., Savel'ev, S. E., Lin, S., Wang, Z., Li, Y., Joshi, S., Midya, R., Li, C., Rao, M., et al. (2017). A novel true random number generator based on a stochastic diffusive memristor. *Nature communications*, 8(1):882.

Johansson, T. and Jönsson, F. (1999). Improved fast correlation attacks on stream ciphers via convolutional codes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 347–362. Springer.

Joseph, N. S. P. K. B. (2000). Chaos for stream cipher. *Proc. of Recent Advances in Computing and Communications, Tata McGraw-Hill*, pages 35–42.

Kaur, T. and Sharma, R. (2013). Tj-aca: An advanced cryptographic algorithm for color images using ikeda mapping. *International Journal of Computer Trends and Technology (IJCTT)*, 4(5):1295–1300.

Kendall, M. G. and Smith, B. B. (1938). Randomness and random sampling numbers. *Journal of the royal Statistical Society*, 101(1):147–166.

Khan, J., Ahmad, J., and Hwang, S. O. (2015). An efficient image encryption scheme based on: Henon map, skew tent map and s-box. In *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*, pages 1–6. IEEE.

Kim, Y.-S., Jang, J.-W., and Lim, D.-W. (2010). Linear corrector overcoming minimum distance limitation for secure trng from (17, 9, 5) quadratic residue code. *ETRI journal*, 32(1):93–101.

Knuth, D. E. (1997). *The art of computer programming*, volume 3. Pearson Education.

Kocarev, L. and Jakimoski, G. (2001). Logistic map as a block encryption algorithm. *Physics Letters A*, 289(4):199–206.

Kocarev, L. and Tasev, Z. (2003). Public-key encryption based on chebyshev maps. In *Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*, volume 3, pages III–III. IEEE.

Kohda, T. (2004). Statistical properties of chaotic sequences generated by jacobian elliptic chebyshev rational maps. In *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, volume 5, pages V–V. IEEE.

Kohda, T. and Tsuneda, A. (1993). Pseudonoise sequences by chaotic nonlinear maps and their correlation properties. *IEICE Transactions on Communications*, 76(8):855–862.

Kohda, T. and Tsuneda, A. (1995). Chaotic bit sequences for stream cipher cryptography and their correlation functions. In *Chaotic Circuits for Communication*, volume 2612, pages 86–98. International Society for Optics and Photonics.

Kohda, T. and Tsuneda, A. (1997). Statistics of chaotic binary sequences. *IEEE Transactions on information theory*, 43(1):104–112.

Kotulski, Z., Szczepański, J., Górski, K., Paszkiewicz, A., and Zugaj, A. (1999). Application of discrete chaotic dynamical systems in cryptography—dcc method. *International Journal of Bifurcation and Chaos*, 9(06):1121–1135.

Kuusela, T. (1993). Random number generation using a chaotic circuit. *Journal of Nonlinear Science*, 3(1):445–458.

Kwok, H. and Tang, W. K. (2007). A fast image encryption system based on chaotic maps with finite precision representation. *Chaos, solitons & fractals*, 32(4):1518–1529.

Kwok, S.-H., Ee, Y.-L., Chew, G., Zheng, K., Khoo, K., and Tan, C.-H. (2011). A comparison of post-processing techniques for biased random number generators. In *IFIP International Workshop on Information Security Theory and Practices*, pages 175–190. Springer.

Lacharme, P. (2008). Post-processing functions for a biased physical random number generator. In *Fast Software Encryption*, pages 334–342. Springer.

Lacharme, P. (2009). Analysis and construction of correctors. *IEEE Transactions on Information Theory*, 55(10):4742–4748.

Lambić, D. (2017). Cryptanalyzing a novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, 89(3):2255–2257.

Lasota, A. and Mackey, M. C. (2013). *Chaos, fractals, and noise: stochastic aspects of dynamics*, volume 97. Springer Science & Business Media.

Lehmann, A. E., Filippov, T. V., Sarwana, S. M., Kirichenko, D. E., Dotsenko, V. V., Sahu, A., and Gupta, D. (2017). Embedded rsfq pseudorandom binary sequence generator for multichannel high-speed digital data link testing and synchronization. *IEEE Transactions on Applied Superconductivity*, 27(4):1–6.

Lehmer, D. H. (1951). Mathematical methods in large-scale computing units. *Annu. Comput. Lab. Harvard Univ.*, 26:141–146.

Li, C., Deng, W., and Xu, D. (2006). Chaos synchronization of the chua system with a fractional order. *Physica A: Statistical Mechanics and its Applications*, 360(2):171–185.

Li, C., Li, S., Alvarez, G., Chen, G., and Lo, K.-T. (2008). Cryptanalysis of a chaotic block cipher with external key and its improved version. *Chaos, Solitons & Fractals*, 37(1):299–307.

Li, S., Chen, G., and Mou, X. (2005). On the dynamical degradation of digital piecewise linear chaotic maps. *International Journal of Bifurcation and Chaos*, 15(10):3119–3151.

Li, S., Li, Q., Li, W., Mou, X., and Cai, Y. (2001a). Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. In *IMA International Conference on Cryptography and Coding*, pages 205–221. Springer.

Li, S., Mou, X., Cai, Y., Ji, Z., and Zhang, J. (2003). On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. *Computer physics communications*, 153(1):52–58.

Li, S., Mou, X., and Cai, Y.-L. (2001b). Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. In *Progress in Cryptology–INDOCRYPT 2001: Second International Conference on Cryptology in India Chennai, India, December 16 C20, 2001 Proceedings*, pages 316–329.

Li, T.-Y. and Yorke, J. A. (1975). Period three implies chaos. *The American Mathematical Monthly*, 82(10):985–992.

Lidl, R. and Niederreiter, H. (1997). *Finite fields*, volume 20. Cambridge university press.

Liu, L., Miao, S., Hu, H., and Deng, Y. (2016). Pseudorandom bit generator based on non-stationary logistic maps. *IET Information Security*, 10(2):87–94.

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the atmospheric sciences*, 20(2):130–141.

Lozi, R. (2012). Emergence of randomness from chaos. *International Journal of Bifurcation and Chaos*, 22(02):1250021.

Lü, J. and Chen, G. (2002). A new chaotic attractor coined. *International Journal of Bifurcation and chaos*, 12(03):659–661.

Lu, J., Wu, X., and Lü, J. (2002). Synchronization of a unified chaotic system and the application in secure communication. *Physics letters A*, 305(6):365–370.

MacLaren, M. D. and Marsaglia, G. (1965). Uniform random number generators. *Journal of the ACM (JACM)*, 12(1):83–89.

MacWilliams, F. J. and Sloane, N. J. A. (1977). *The theory of error-correcting codes*. Elsevier.

Mandi, M., Haribhat, K., and Murali, R. (2010). Generation of large set of binary sequences derived from chaotic functions defined over finite field gf (28) with good linear complexity and pairwise cross correlation properties. *Inter. Jour. of Distributed and Parallel systems*, 1(1):93–112.

Markovski, S., Gligoroski, D., and Kocarev, L. (2005). Unbiased random sequences from quasigroup string transformations. In *International Workshop on Fast Software Encryption*, pages 163–180. Springer.

Márton, K., Pârvu, L., and Suciu, A. (2018). The impact of post-processing functions on random number sequences. In *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pages 1–6. IEEE.

Matsumoto, M. and Nishimura, T. (1998). Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 8(1):3–30.

Matsumoto, M., Nishimura, T., Hagita, M., and Saito, M. (2005). Cryptographic mersenne twister and fubuki stream/block cipher. *IACR Cryptology ePrint Archive*, 2005:165.

Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13(1):29–42.

Meier, W. and Staffelbach, O. (1988). Fast correlation attacks on stream ciphers. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 301–314. Springer.

Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

Meranza-Castillón, M., Murillo-Escobar, M., López-Gutiérrez, R., and Cruz-Hernández, C. (2019). Pseudorandom number generator based on enhanced hénon map and its implementation. *AEU-International Journal of Electronics and Communications*, 107:239–251.

Michalak, K. P. (2014). How to estimate the correlation dimension of high-dimensional signals? *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 24(3):033118.

Murillo-Escobar, M., Cruz-Hernández, C., Cardoza-Avendaño, L., and Méndez-Ramírez, R. (2017). A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, 87(1):407–425.

Nejati, H., Beirami, A., and Ali, W. H. (2012). Discrete-time chaotic-map truly random number generators: design, implementation, and variability analysis of the zigzag map. *Analog Integrated Circuits and Signal Processing*, 73(1):363–374.

Nishimura, T. (2000). Tables of 64-bit mersenne twisters. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 10(4):348–357.

Oliver, N., Soriano, M. C., Sukow, D. W., and Fischer, I. (2013). Fast random bit generation using a chaotic laser: approaching the information theoretic limit. *IEEE Journal of Quantum Electronics*, 49(11):910–918.

Özkaynak, F. and Özer, A. B. (2010). A method for designing strong s-boxes based on chaotic lorenz system. *Physics Letters A*, 374(36):3733–3738.

Pain, P., Das, K., Sadhu, A., Kanjilal, M. R., and De, D. (2019). Novel true random number generator based hardware cryptographic architecture using quantum-dot cellular automata. *International Journal of Theoretical Physics*, pages 1–20.

Palit, S. and Bimal, K. (2004). Some statistical attacks on stream cipher cryptosystems. *Journal of Indian Statistical Association*, 42:1–34.

Palmore, J. and Herring, C. (1990). Computer arithmetic, chaos and fractals. *Physica D: Nonlinear Phenomena*, 42(1-3):99–110.

Pareek, N., Patidar, V., and Sud, K. (2003). Discrete chaotic cryptography using external key. *Physics Letters A*, 309(1):75–82.

Pareek, N., Patidar, V., and Sud, K. (2005). Cryptography using multiple one-dimensional chaotic maps. *Communications in Nonlinear Science and Numerical Simulation*, 10(7):715–723.

Pareschi, F., Rovatti, R., Setti, G., et al. (2006). Simple and effective post-processing stage for random stream generated by a chaos-based rng. In *Proceedings of NOLTA*, pages 383–386.

Park, S. K. and Miller, K. W. (1988). Random number generators: good ones are hard to find. *Communications of the ACM*, 31(10):1192–1201.

Pecora, L. M. and Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical review letters*, 64(8):821.

Peinado, A. and Fúster-Sabater, A. (2013). Generation of pseudorandom binary sequences by means of linear feedback shift registers (lfsrs) with dynamic feedback. *Mathematical and Computer Modelling*, 57(11-12):2596–2604.

Persohn, K. and Povinelli, R. J. (2012). Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. *Chaos, Solitons & Fractals*, 45(3):238–245.

Petrie, C. S. and Connelly, J. A. (2000). A noise-based ic random number generator for applications in cryptography. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 47(5):615–621.

Phatak, S. and Rao, S. S. (1995). Logistic map: A possible random-number generator. *Physical review E*, 51(4):3670.

Pichler, F. and Scharinger, J. (1996). Finite dimensional generalized baker dynamical systems for cryptographic applications. In *Computer Aided Systems Theory—EUROCAST'95*, pages 465–476. Springer.

Rössler, O. E. (1976). An equation for continuous chaos. *Physics Letters A*, 57(5):397–398.

Rueppel, R. A. (1986). Stream ciphers. In *Analysis and Design of Stream Ciphers*, pages 5–16. Springer.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., and Barker, E. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va.

Said, M. R. M., Hina, A. D., and Banerjee, S. (2017). Cryptanalysis of a family of 1d unimodal maps. *The European Physical Journal Special Topics*, pages 1–17.

Šajić, S., Maletić, N., Todorović, B. M., and Šunjevarić, M. (2013). Random binary sequences in telecommunications. *Journal of Electrical Engineering*, 64(4):230–237.

Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, 5(1):3–55.

Shujun, L., Xuanqin, M., and Yuanlong, C. (2001). Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In *International Conference on Cryptology in India*, pages 316–329. Springer.

Shukla, R. (2007). *Fast correlation attack on stream cipher*. PhD thesis, Indian Statistical Institute, Kolkata.

Sidelnikov, V. M. (1971). On the mutual correlation of sequences. In *Soviet Math. Dokl.*, volume 12, pages 197–201.

Siegenthaler, T. (1984). Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.). *IEEE Transactions on Information theory*, 30(5):776–780.

Siegenthaler, T. (1985). Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on computers*, 1(C-34):81–85.

Siripragada, A., Prasad, R. S., and Mohankumar, N. (2019). Power efficient puf-based random reseeding true random number generator. In *Soft Computing and Signal Processing*, pages 549–559. Springer.

Skrobek, A. (2007). Cryptanalysis of chaotic stream cipher. *Physics Letters A*, 363(1-2):84–90.

Soleymani, A., Nordin, M. J., and Sundararajan, E. (2014). A chaotic cryptosystem for images based on henon and arnold cat map. *The Scientific World Journal*, 2014.

Soorat, R., Vudayagiri, A., et al. (2015). Hardware random number generator for cryptography. *arXiv preprint arXiv:1510.01234*.

Stinson, D. R. (2005). *Cryptography: theory and practice*. CRC press.

Stojanovski, T., Pihl, J., and Kocarev, L. (2001). Chaos-based random number generators. part ii: practical realization. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 48(3):382–385.

Sudheer, K. S. and Sabir, M. (2011). Adaptive modified function projective synchronization of multiple time-delayed chaotic rossler system. *Physics Letters A*, 375(8):1176–1178.

Sun, F. and Liu, S. (2009). Cryptographic pseudo-random sequence from the spatial chaotic map. *Chaos, Solitons & Fractals*, 41(5):2216–2219.

Sunar, B., Martin, W. J., and Stinson, D. R. (2007). A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on computers*, 56(1).

Tang, H., Qin, T., Hui, Z., Cheng, P., and Bai, W. (2018). Design and implementation of a configurable and aperiodic pseudo random number generator in fpga. In *2018 IEEE 2nd International Conference on Circuits, System and Simulation (ICCSS)*, pages 47–51. IEEE.

Tang, K. and Tang, W. (2006). A low cost chaos-based random number generator realized in 8-bit precision environment. In *Proceedings of 2006 International Symposium in Nonlinear Theory and its Applications*, pages 395–398.

Tang, X., Udaya, P., and Fan, P. (2007). Generalized binary udaya–siddiqi sequences. *IEEE transactions on information theory*, 53(3):1225–1230.

Tao, S., Ruli, W., and Yixun, Y. (1998). Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters*, 34(9):873–874.

Tavas, V., Demirkol, A. S., Ozoguz, S., Kilinc, S., Toker, A., and Zeki, A. (2010). An ic random number generator based on chaos. In *Applied Electronics (AE), 2010 International Conference on*, pages 1–4. IEEE.

Taylor, G. and Cox, G. (2011). Digital randomness. *IEEE spectrum*, 48(9):32–58.

Theiler, J. (1987). Efficient algorithm for estimating the correlation dimension from a set of discrete points. *Physical review A*, 36(9):4456.

Tian, X. and Benkrid, K. (2009). Mersenne twister random number generation on fpga, cpu and gpu. In *Adaptive Hardware and Systems, 2009. AHS 2009. NASA/ESA Conference on*, pages 460–464. IEEE.

Tsuneda, A., Eguchi, K., and Inoue, T. (1999). Design of chaotic binary sequences with good statistical properties based on piecewise linear into maps. In *Microelectronics for Neural, Fuzzy and Bio-Inspired Systems, 1999. MicroNeuro'99. Proceedings of the Seventh International Conference on*, pages 261–266. IEEE.

Tsuneda, A., Mitsuishi, S., and Inoue, T. (2007). A study on generation of random bit sequences with post-processing by linear feedback shift registers. In *Innovative Computing, Information and Control, 2007. ICICIC'07. Second International Conference on*, pages 92–92. IEEE.

Vlassopoulos, N. and Girau, B. (2014). A metric for evolving 2-d cellular automata as pseudo-random number generators. *Journal of Cellular Automata*, 9.

Von Neumann, J. (1951). Various techniques used in connection with random digits. *Applied Math Series*, 12(36-38):1.

Wah, T, K. (2007). *Chaos-based random number generator in finite precision environment*. PhD thesis, City University of Hong Kong.

Wang, L., Wang, D., Li, P., Guo, Y., Zhao, T., Wang, Y., and Wang, A. (2018). Post-processing-free multi-bit extraction from chaotic laser diode with cfbg feedback. *IEEE Photonics Technology Letters*, 30(16):1435–1438.

Wang, X.-Y., Yang, L., Liu, R., and Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics*, 62(3):615–621.

Wang, Y., Hui, C., Liu, C., and Xu, C. (2016). Theory and implementation of a very high throughput true random number generator in field programmable gate array. *Review of Scientific Instruments*, 87(4):044704.

Welch, L. (1974). Lower bounds on the maximum cross correlation of signals (corresp.). *IEEE Transactions on Information theory*, 20(3):397–399.

Wheeler, D. D. (1989). Problems with chaotic cryptosystems. *Cryptologia*, 13(3):243–250.

Wheeler, D. D. and Matthews, R. A. (1991). Supercomputer investigations of a chaotic encryption algorithm. *Cryptologia*, 15(2):140–152.

Wicker, S. B. (1995). *Error control systems for digital communication and storage*, volume 1. Prentice hall Englewood Cliffs.

Wong, K.-W., Ho, S.-W., and Yung, C.-K. (2003). A chaotic cryptography scheme for generating short ciphertext. *Physics Letters A*, 310(1):67–73.

Wong, W.-k., Lee, L.-p., and Wong, K.-w. (2001). A modified chaotic cryptographic method. *Computer Physics Communications*, 138(3):234–236.

Xiao, G.-Z. and Massey, J. L. (1988). A spectral characterization of correlation-immune combining functions. *IEEE Transactions on information theory*, 34(3):569–571.

Yang, Y.-G. and Zhao, Q.-Q. (2016). Novel pseudo-random number generator based on quantum random walks. *Scientific reports*, 6:20362.

Zhang, J., Wang, Y., Liu, M., Xue, L., Li, P., Wang, A., and Zhang, M. (2012). A robust random number generator based on differential comparison of chaotic laser signals. *Optics express*, 20(7):7496–7506.

Zheng, F., Tian, X.-j., Song, J.-y., and Li, X.-Y. (2008). Pseudo-random sequence generator based on the generalized henon map. *The Journal of China Universities of Posts and Telecommunications*, 15(3):64–68.

Zhou, H. and Ling, X.-T. (1997). Problems with the chaotic inverse system encryption approach. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, 44(3):268–271.

Zhou, H., Ling, X.-T., and Yu, J. (1997). Secure communication via one-dimensional chaotic inverse systems. In *Circuits and Systems, 1997. ISCAS'97., Proceedings of 1997 IEEE International Symposium on*, volume 2, pages 1029–1032. IEEE.

Zidan, M. A., Radwan, A. G., and Salama, K. N. (2011). Random number generation based on digital differential chaos. In *Circuits and Systems (MWSCAS), 2011 IEEE 54th International Midwest Symposium on*, pages 1–4. IEEE.

BIODATA OF STUDENT

The student, ALIYU DANLADI HINA, was born in July 1975 at Hinna Yamaltu/Deba Local Government of Gombe State, Nigeria. He received a B.Tech (Mathematics) and M.Sc (Mathematics) from Abubakar Tafawa Balewa University Bauchi-Nigeria. His research interests includes Number theory, Dynamical systems, chaos theory and cryptography (key generation and analysis). He is married and blessed with three children - Al'ameen, Fatima (Afrah) and Abubakar. He is currently a lecturer with The federal Polytechnic, Bauchi-Nigeria. The student can be reached via email address; dhaliyu@fptb.edu.ng.

LIST OF PUBLICATIONS

The following are the list of publications that arise from this study.

A. D. Hina, Mohamed Rushdan. MD Said, Santo Banerjee (2015). Chaotic Pseudorandom Sequences and the Security of Cryptosystems. *Springer Proceedings in Complexity: Chaos Complexity and Leadership*. 2013: 163 – 174.

Mohamed Rushdan Md Said., **A. D. Hina**, Santo Banerjee (2017). Cryptanalysis of a family of 1D unimodal maps. *European Physical. Journal. Special Topics 226*. 2281-2297.

UNIVERSITI PUTRA MALAYSIA
STATUS CONFIRMATION FOR THESIS/PROJECT REPORT AND COPYRIGHT
ACADEMIC SESSION: Second Semester 2018/2019

TITLE OF THE THESIS/PROJECT REPORT:
GENERATION AND STATISTICAL ANALYSIS OF CHAOS-BASED PSEUDORANDOM SEQUENCES

NAME OF STUDENT: ALIYU DANLADI HINA

I acknowledge that the copyright and other intellectual property in the thesis/project report belonged to Universiti Putra Malaysia and I agree to allow this thesis/project report to be placed at the library under the following terms:

1. This thesis/project report is the property of Universiti Putra Malaysia.
2. The library of Universiti Putra Malaysia has the right to make copies for educational purposes only.
3. The library of Universiti Putra Malaysia is allowed to make copies of this thesis for academic exchange.

I declare that this thesis is classified as:

*Please tick(✓)

☐	CONFIDENTIAL	(contain confidential information under Official Secret Act 1972).
☐	RESTRICTED	(Contains restricted information as specified by the organization/institution where research was done).
☐	OPEN ACCESS	I agree that my thesis/project report to be published as hard copy or online open access.

This thesis is submitted for:

☐	PATENT	Embargo from _____(date) until _____(date).

Approved by:

_____	_____
(Signature of Student)	(Signature of Chairman of Supervisory Committee)
Passport No.:A05771429	Name: **Mohamad Rushdam MD Said, PhD**
Date:	Date:

[Note: If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization/institution with period and reasons for confidentially or restricted.]