Use of Chaotic Number Generators for Random Number Generation

by

Abdul Basit

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

Sep 2019

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Abdul Basit**, Registration No. **00000240994**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: _____
Name of Supervisor **Dr. Mehreen Afzal**
Date: _____

Signature (HOD): _____
Date: _____

Signature (Dean/Principal) _____
Date: _____

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

Dedication

“In the name of Allah, the most Beneficent, the most Merciful"

I dedicate this thesis to my parents, family and teachers who supported me each step of the way.

v

Abstract

Chaos is a mathematical branch which focuses on dynamic systems and studies their behavior. It is a theory that is interdisciplinary and describes that there are some patterns, self- similarities, repetitions, feedback loops which are constant, fractals and it relies on programming at the starting point which is sensitive to initial conditions. Chaos is something in between predictable and unpredictable. It has also been in practice for last two decades in cryptography. Hundreds of cryptographic primitives have been designed by using chaos and nonlinear dynamics which include both symmetric and asymmetric encryption schemes. Their aperiodic behavior attracted researchers to develop different encryption algorithms achieving confusion and diffusion by utilizing the properties of these maps. Despite of many advantages the cryptographic security of these schemes is still questionable. Specially with the increase in computer resources the adversary always considered with added advantage in terms of resources and technology. Quantum computation is also one of the latest developing technology which has threatened the classical cryptography. This thesis will give analysis of chaos-based cryptography while analyzing the cryptographic properties of these maps and future of chaos-based cryptography in post quantum era.

Acknowledgments

All praises to Allah for the strengths and His blessing in completing this thesis.

I would like to convey my gratitude to my supervisor, Dr. Mehreen Afzal, for her supervision and constant support. Her invaluable help of constructive comments and suggestions throughout the thesis works are major contributions to the success of this research. Also, I would thank my committee members; Asst Prof Dr. Fawad Khan, and Asst Prof Mian Muhammad Waseem Iqbal for their support and knowledge regarding this topic.

Abdul Basit

Table of Contents

THESIS ACCEPTANCE CERTIFICATE ii

ABSTRACT v

ACKNOWLEGEMENTS vi

LIST OF FIGURES ix

LIST OF TABLES x

ACRONYMS xi

1 Introduction 1
1.1 Overview. 1
1.2 Motivation and Problem Statement 2
1.3 Objectives 3
1.4 Thesis Organization 3

2 Introduction to Chaos Theory 5
2.1 Introduction 5
2.2 Attractors 5
2.2.1 Types of Attractors 5
2.3 Chaos in Cryptography 7
2.3.1 Logistic Map 7

3 Chaotic Maps for Random Number Generation 9
3.1 Introduction 9
3.2 Randomness Testing Criterion 9
3.2.1 DIEHARD Test 9
3.2.2 ENT Test 11
3.2.3 TestU01 11
3.2.4 NIST SP 800-22 11
3.3 Overview 12
3.3.1 Henon Map 13
3.3.2 Chebyshev Polynomial and Tinkerbell Map 15
3.3.3 Quantum Logistic Map 15
3.3.4 Chaotic Map Using Linear Feedback Shift Register 17
3.3.5 Billiard Map 18
3.4 PRNGs other than Chaotic Maps 19
3.5 Conclusion 20

4 Framework for Analysis of Chaotic Map 21
4.1 Introduction 21
4.2 Chaotic Region Determination 21
4.2.1 Lyapunov Exponent 21
4.2.2 Bifurcation Diagram 22

4.3 Improvised Chaotic Map 25
4.4 Conclusion 27

5 Cryptographic Properties of Chaotic Maps 28
5.1 Introduction 28
5.2 Speed of Chaotic Maps 28
5.3 Key Space 29
5.4 Analysis 36
5.4.1 Advantages of Chaos – Based Cryptography 40
5.4.2 Limitations of Chaos – Based Cryptography 41
5.5 Design Criterion for Chaos – Based Cryptography 43

6 Chaos – Based PKC in Post Quantum Era 45
6.1 Introduction 45
6.2 Overview 45
6.3 Quantum Computers and Cryptography 47
6.4 Conclusion 48

7 Conclusion 49

Bibliography 51

List of Figures

1.1	Lorenz Attractor	2
2.1	Fixed Point Attractor.	5
2.2	Closed – Curved Attractor.	6
2.3	Torus Attractor.	6
2.4	Strange Attractor	7
2.5	Iterative Function for Logistic Map.	8
3.1	Strange Attractor of Henon	14
3.2	Bifurcation Diagram for Quantum Map	17
4.1	Lyapunov Exponent	26
4.2	Saddle – Node Bifurcation	27
4.3	Transcritical Bifurcation	27
4.4	Pitchfork Bifurcation.	28
4.5	Bifurcation Diagram for Lorenz Equation	28
4.6	Time evolution Diagram for Improvised K - Logistic Map	29
4.7	Bifurcation and Zigzag Diagram for K – Logistic Map	30
4.8	Lyapunov Exponent for K – Logistic Map	31
5.1	Mean Squared Error between two 32-bit processors	33
5.2	Combined Plot of Lyapunov and Bifurcation for Logistic Map	34
5.3	Coweb Plot for Stable Fixed Point	35
5.4a	Coweb Plot for Periodic Region	35
5.4b	Coweb Plot for Chaotic Region	36
5.5a	Coweb Plot for r = 3.83	36
5.5b	Coweb Plot for r = 3.85	37
5.6	LE Diagram for r = 3.9 to 4 with difference of 2 decimals….	38
5.7	LE Diagram for r = 3.9 to 4 with difference of 3 decimals….	39
5.8	LE Diagram for r = 3.9 to 4 with difference of 4 decimals….	39
5.9	Complete chaotic region with r = 3.57 – 4 with 1 decimal place	40

List of Tables

3.1 Different Pseudo-Random Number Generators 24

5.1 Key Space Calculation of Logistic Map By varying decimal . . . . . .38 places of *x* and *r*

5.2 Different Cycles for Logistic Map 42

ACRONYMS

Definition	Acronym
Federal Information Processing Standards	FIPS
National Institute of Standards and Technology	NIST
Pseudo Random Number Generator	PRNG
Lyapunov Exponent	LE
Public Key Cryptography	PKC
Discrete Logarithm Problem	DLP
Rivest, Shamir and Adleman	RSA
Diffie – Hellman	DH
Iterative Functions	IF
Man in the Middle	MITM
Advance Encryption Standard	AES
Elliptic Curve Digital Signature Algorithm	ECDSA
Short Vector Problem	SVP
Sum of Absolute Difference	SAD

Chapter 1

Introduction

1.1 Overview

Prediction of systems has always been an attraction for scientists for futuristic planning. For examples, eclipse dates can be calculated for past and future both. Yet there are systems which are unpredictable and generate random behavior, but still fall under the laws of physics. Such examples are roll of dice, flow of streams and weather etc. However, in recent past scientists realized that there are certain deterministic systems which can generate random behaviors. These systems are known as chaotic systems.

Scientists have worked a lot to explore the hidden truth of this universe. Astronomers used Newton's Law to detect the future position of planets and comets. Meteorologists used previous data to forecast weather. But they never included every particle of the atmosphere to calculate everything, rather they were specific to data effecting their task.

In 1960 an American meteorologist Edward N. Lorenz created a model for weather forecasting which included twelve equations showing relationship of different factors such as temperature, pressure and wind speed. After every minute his computer printed out a row of numbers that represented a day of weather and his model was following early weather patterns. One day Lorenz decided to repeat the calculations and started the calculations from mid-point, giving inputs from printout. Due to noisy computer he left his seat for a cup of coffee and on his return, he was surprised to see results as they were totally different as compared to earlier printed results. Since same program being used for calculations and all inputs were also from previously calculated data, hence result should have been same. Lorenz saw that computer used six digits number for calculation and printed data was only three digits (0.567891→ 0.567) and due to this change the system behaved differently outputting different result. Lorenz discovered that system was sensitive to initial conditions and this is how he introduced Chaos.

For more analysis of the systems which are sensitive to initial conditions Lorenz simplified the system to three equations and three variables to model convection instead of weather. He obtained hundreds of triplets like (9, 20, 0) and plotted these points as graph. The resulting pattern was like butterfly (Fig. 1.1) and path never repeated itself. The behavior signaled disorder since no path recurred. At same time the behavior signaled order since all the paths were confined in overall pattern. Since each set of initial conditions will result into different path within the overall pattern, Lorenz concluded, "that prediction of sufficiently distant future is impossible by any method, unless the present conditions are known exactly. In view of the inevitable inaccuracy and incompleteness of weather observations, precise very-long-range forecasting would seem to be non-existence" [1].

Fig.1.1 Lorenz Attractor [1]

1.2 Motivation and Problem Statement

Most of the researchers have been working on Pseudo-Chaos, which approximates continuous chaos with floating or fixed-point arithmetic and leads to discrete chaos-like system with low cycle lengths. It is essential that stable pseudo-chaotic systems should have almost the same period and Lyapunov exponents for all possible initial conditions. Majority of the known pseudo-chaotic systems do not fulfill this criterion, but still chaotic systems are being used and hardly research has been done to identify the strength

of chaotic number generators. There is need to identify which essential properties guarantee computational unpredictability of a chaotic system.

Properties of chaotic maps attract researchers for development of different cryptographic schemes but still there are certain limitations for its actual implementations which are required to be identified. Post quantum cryptography will change the cryptographic primitives due to high speed and more storage capacity, especially public key cryptography will come to end with implementation of Shor's Algorithm. There is need of new quantum resistant primitives, can chaos-based cryptography be one out of them.

1.3 Objectives

The main objectives of thesis are: -

- To study the Chaotic theory and its application in cryptography.
- To identify the reasons to use the chaotic number generators as pseudorandom number generators.
- To study framework for analysis of pseudorandom numbers generated by chaotic systems.

1.5 Thesis Organization

The thesis is structured as follows:

- Chapter 2 contains introduction to chaos theory. Different types of attractors and use of chaos theory in cryptography are covered in the chapter.

- Chapter 3 contains the study of different chaotic maps. The randomness testing standards, results of randomness of discussed chaotic maps and their cryptographic properties are discussed in this chapter.

- Chapter 4 covers the framework and techniques to identify the chaotic region and effects of improvisation during implementation of chaotic maps.

- Chapter 5 contains analysis of cryptographic properties of chaotic maps. It also contains results after analysis of key space generated by logistic map and effects of decimal number arithmetic on speed and key space.

- Chapter 6 contains post quantum cryptography effects on public key cryptography and effectiveness of chaos-based cryptography.

- Chapter 7 marks the end of the document. The conclusion and future of chaos-based cryptography are suggested in this chapter.

Chapter 2

Introduction to Chaos Theory

2.1 Introduction

Science uses the terms chaos and disorder, along with the term nonrandom and degree of predictability makes these terms distinguishable. A nonrandom process is predictable as compared to random process which is totally unpredictable. A chaotic process falls in between these two extremes of total predictability and total unpredictability. Reason for this is that equations can be written to describe the behavior of chaotic systems, hence predictable theoretically. Yet unpredictable in practice since being predictable temporarily. This chapter will include different types of attractors and use of chaos theory in cryptography.

2.2 Attractors

As compared to static systems, dynamic systems have constant changing conditions. Scientists graph the changing values of system variables to observe the behavior of dynamic systems. The resulting graph is known as phase space which is plot of system over time. With the time the graph settles into a shape which is known as attractor. So, one can say the dynamic behavior is attracted to this geometric shape.

2.2.1 Types of Attractors. There are four types of attractors.

Fixed point Attractors. In which a moving body comes back to a fixed point. This fixed point is an attractor for that body. Example is a swing which move back and forth and eventually comes to rest at a fixed point as shown in Fig. 2.1.

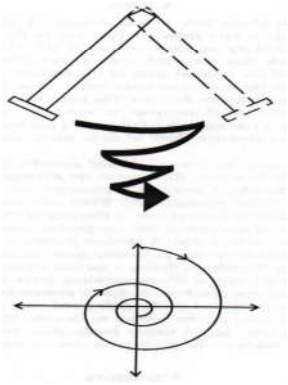

Fig. 2.1 Fixed Point Attractor [1]

Closed – Curved Attractor. Not all attractors are fixed point, some are cyclic like pendulum. A clock pendulum repeats its swing and its attractor is known as closed curve Fig. 2.2. Another example of closed curve attractor is orbit of moon.

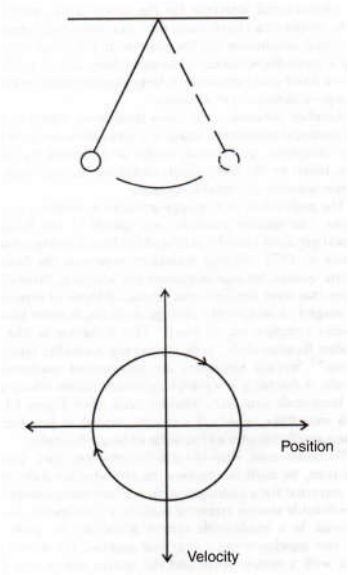

Fig. 2.2 Closed Curve Attractor [1]

A system can have more than one attractor depending upon its initial condition. A small displaced pendulum would not repeat its swing and will come to rest hence fixed-point attractor, while a largely displaced pendulum will follow closed curve attractor.

Torus Attractor. It is a system which change in detailed characteristic over time but does not change its form. Such a system has trajectory which will produce a path looking like the doughnut shape of a torus Fig 2.3.

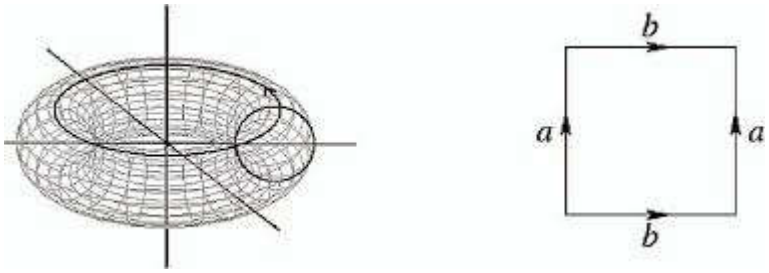

Fig. 2.3 Torus Attractor [1]

It is seen in certain electrical oscillators. The paths taken by fixed- point, closed curve and torus attractors are not sensitive to initial conditions.

Strange Attractors. These attractors are sensitive to initial conditions and known as chaotic attractors. These follow the butterfly path as shown in Fig. 2.4

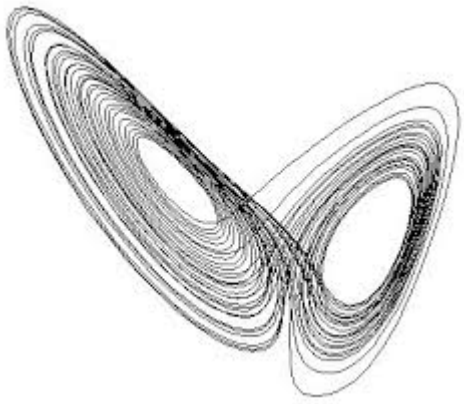

Fig. 2.4 Strange Attractor [1]

Why chaotic systems lose their predictability with time, one needs to study attractors to answer this question. Because a predictable system will not have randomness property and will lose its effect in cryptography.

2.3 Chaos in Cryptography

Sensitive dependence or sensitive to initial conditions property in chaotic systems is very important for cryptography. If initial conditions for the encryption of data is changed by a small value, the resulted encryption would result into totally a different data. Pseudo random numbers have always been an interest for cryptographic algorithm developers since they provide unique keys and be regenerated at both ends (encryption and decryption). However, it has also been a research topic to produce PRNG proving to be computationally secure with maximum period.

2.3.1 Logistic Map

In 1998 M.S. Baptista used ergodic property of low – dimensional and simple logistic map to encrypt a message [2].

$$X_{n+1} = b\, X_n\, (1- X_n) \qquad (1)$$

Where $X_n \in [0,1]$, for a control parameter b which set to be 3.78 which gives maximum points without repetition. But later in 2008 [3] the writer proved inadequacy for use of logistics map for cryptographic applications due to reason that logistic map is unimodal. Figure 2.5 show the unimodal behavior for the iterative function of logistics map. When x = 0.5 the function reaches to its maximum value and it is monotonically increasing and decreasing for x<0.5 and

x> 0.5 respectively. Their study in [3] showed that; (a) there exists a periodic window in bifurcation diagram of logistic map and effecting the key space. (b) if the probability density function distribution of logistic map is analyzed then it is revealed that it's not uniform and resulting into very slow encryption speed. (c) chaotic orbit of logistic map is very important to hide encrypted text (ciphertext) so that one cannot get plaintext or secret key. But in logistic map the extreme value for function is at x = 0.5 (λ/4). It is possible to get chaotic orbit with known plaintext attack and then by using the function one can get control parameters. Even if the ciphertext is resulted by best random process, with enough large samples of ciphertext one can guess value of λ by using maximum value in ciphertext. (d) critical points of logistic map are independent of control parameters. Known plaintext attack can be launched for reconstruction of symbolic sequences associated with secret value of λ. (e) chosen plaintext attack can be launched by using return map hence revealing the value of λ, since return map is dependent upon control parameters in logistic map. (f) statistical complexity of the logistic map is almost bijective of the control parameters which can be exploited by the cryptanalysis.

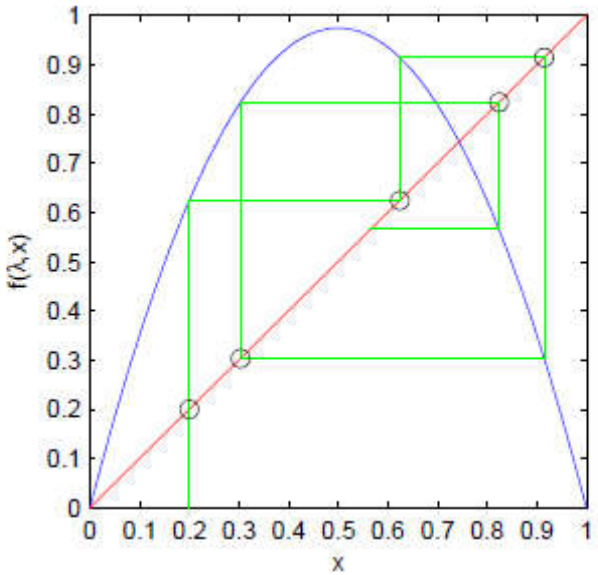

Fig.2.5 Iterative function for logistic map [3]

Chapter 3

Chaotic Maps for Random Number Generators

3.1 Introduction

This chapter includes survey of chaotic maps. Existing randomness testing criterion are also discussed prior to give survey since these chaotic maps are used for random number generation and tested against these testing criteria.

3.2 Randomness Testing Criteria

After 2000 researchers worked to create pseudorandom number using pseudo chaos. However, people were already working to develop some theoretical, empirical and statistical testing standards and programs to check the randomness of the PRNGs. Earlier researchers used Menezes et al basic tests of randomness developed in 1997, having tests like auto – correlation, frequency, run, poker and serial. A threshold value was selected for comparison of each test result, it is one sided test. FIPS 140-1 also recommended some batteries of tests which includes run, long run, monobit and poker. FIPS 140 – 1 is two-sided test where statistics of a test are required to lie within interval. Later, many other tests were also introduced and currently most renown randomness test are:

1. Diehard Test
2. ENT Test
3. TestU01
4. NIST standard SP800-22

3.2.1 Diehard Test

It is a statistical test developed by George Marsaglia in 1995, which contains following test to check the randomness quality:

1. **Birthday Spacing**. the test is based on birthday paradox, performed on PRNGs by choosing random points on large intervals.
2. **Overlapping Permutation**. A sequence of five consecutive PRNs is chosen for analysis, one million random integers of length 32 bits should have 120 states. these 120 states should occur with qual probability.

3. **Ranks of Matrices**. also known as Chi square test, which is performed on 31 x 31 matrix formed by 31 leftmost bits of 31 integers belong to random numbers, and rank is determined. Chi square test is performed to determine the counts of ranks 31, 30, 29 and less than or equal to 28. the same test is performed for 32 x 32 matrix and 6 x 8 matrix as well.
4. **Monkey Test**. it is based upon infinite monkey theorem, performed on a stream of bits to count the overlapping words.
5. **Count the 1s**. Number of 1s are counted in each of either successive or selected bytes. this count is converted into letters and then how many five letter words occurred is determined.
6. **Parking Lot Test**. in 100 x 100 square a unit circle is randomly parked. a successful parking is that in which parking circle does not overlap already parked circle. these parked circles should follow normal distribution at least after 12,000 tries.
7. **Minimum Distance Test**. 8000 points are randomly placed in a 10000×10000 square, then minimum distance in between the pairs is determined. there should be exponential distribution with a mean when square of this distance is plotted.
8. **Random Spheres Test**. a cube having 1000 edges is chosen and randomly 4000 points are picked from it. a sphere having radius equal to minimum distance from another point is centered on each point. The smallest sphere's volume should be exponentially distributed.
9. **The Squeeze Test**. it is 100000 times repeated test in which 2^{31} is multiplied by random floats on (0,1) till the time it appears 1 and these number of floats required to reach to 1 should follow a certain distribution.
10. **Overlapping Sums Test**. a long sequence of random floats on (0,1) is generated and consecutive 100 floats are added up. this sum should be normally distributed with some variance and mean.
11. **Runs Test**. A long sequence of random floats on (0,1) is counted for ascending and descending runs which should follow a certain distribution.
12. **The Craps Test**. 200000 games of craps are played, and number of wins number of throws as well are counted.

p-value is returned by most of these tests of DIEHARD. these p-values should be uniform on [0,1] provided input file with random bits. if p-value is near to 0 or 1 then bit stream fails randomness test. since these tests are good in numbers hence one will get p< 0.025 and p>0.975. these values mean RNG failed tests but since DIEHARD would produce so many p values and hundreds of these values would not affect randomness of RNGs.

3.2.2 ENT Test

ENT performs six tests on input file containing bit streams and produces following outputs:

1. **Entropy** = 7.980627 bits per character.
2. **Optimum compression** would reduce the size of this 51768 characters file by 0 percent.
3. **Chi square distribution** for 51768 samples is 1542.26, and randomly would exceed this value less than 0.01 percent of the times.
4. **Arithmetic mean** value of data bytes is 125.93 (127.5 = random).
5. **Monte Carlo** value for Pi is 3.169834647 (error 0.90 percent).
6. **Serial correlation coefficient** is 0.004249 (totally uncorrelated = 0.0).

3.2.3 TestU01

It is ANSIC C library which performs number of batteries of tests including small crush (10 tests), Crush (96 tests0 and Big Crush (160 Tests). On a computer with an AMD Athlon 64 processor running at 2.4 GHz, timings for these tests are 14 seconds, 1 hour, and 5.5 hours respectively. TestU01 takes 32 bits input, hence for 64 bits RNG the test required to be performed in two halves for upper and lower bits.

3.2.4 NIST SP 800-22

It is a statistical package which performs 15 tests as following to check the randomness:

1. The Frequency or Monobit Test
2. Frequency Test within a Block

3. The Runs Test
4. Tests for the Longest-Run-of-Ones in a Block
5. The Binary Matrix Rank Test
6. The Discrete Fourier Transform (Spectral) Test
7. The Non-overlapping Template Matching Test
8. The Overlapping Template Matching Test
9. Maurer's "Universal Statistical" Test
10. The Linear Complexity Test
11. The Serial Test
12. The Approximate Entropy Test
13. The Cumulative Sums (Cusums) Test
14. The Random Excursions Test, and
15. The Random Excursions Variant Test.

All these tests return p- value, if the p – value <0.01 then it is concluded that sequence is non -random otherwise random.

3.3 Overview

In 2001 Anger Fog gave concept of Chaotic Random Number Generators with Random Cycle Lengths [4]. Some researchers proved PRNGs as to be good on basis of hidden structure, but if the structure is not tested with all possibilities and flexibility an adversary can have then it is hard to claim that the random number generator is mathematically interactable. Hence Anger Fog emphasized two main properties for PRNGs which required to be tested as randomness and cycle. For checking the both he suggested the self-test code as RANROT generator which has four different types. Type A rotates bits after addition, type B rotates bits before addition, in type B3 more than two terms are included and whereas there is another type W part of bitstreams are rotated separately. In this research paper he introduced chaotic behavior as desired quality of good random numbers. Bifurcation is the most distinct characteristic of the chaotic systems which shows divergence of trajectories with very little difference in starting points. And to measure bifurcation the Lyapunov exponent λ is used. Although Anger Fog did not use

any chaotic mapping in this generator but just used chaotic behavior as testing parameter for his RANDROT generator.

3.3.1 Henon Map

In 2009 Madhekar Suneel used 2D logistics Map instead of 1D as suggested by Lorenz to create pseudorandom numbers which is known as Chaotic Henon Map [5]. Two-dimensional state equations were given by Henon in 1976, these equations represent discrete-time nonlinear dynamical system and expressed as (2).

$$X_{k+1} = -\alpha X^2_k + y_k + 1 \qquad (2)$$
$$y_{k+1} = \beta X_k$$

Figure 3.1 shows the plane diagram of above equations where $\alpha = 1.4$ and $\beta = 0.3$ representing henon attractor as form of strange attractor. States of this mapping is represented in {0,1} to get pseudorandom binary sequence, b_x and b_y two binary bits are obtained as following:

$$b_x = \begin{cases} 1 & \text{if } x > \tau x \\ 0 & \text{if } x \leq \tau x \end{cases}$$

$$b_y = \begin{cases} 1 & \text{if } y > \tau y \\ 0 & \text{if } y \leq \tau y \end{cases}$$

Where τx and τy are thresholds for state variables x and y and chosen as median of large number of consecutive values of x and y respectively such that likelihood of $x > \tau x$ is equal to likelihood of $x \leq \tau x$ for x and same condition applies for y. Hence two-bit streams are obtained from these as bx and by. Then every Pth bit of these two streams is picked to form new bitstreams as Bx and By.

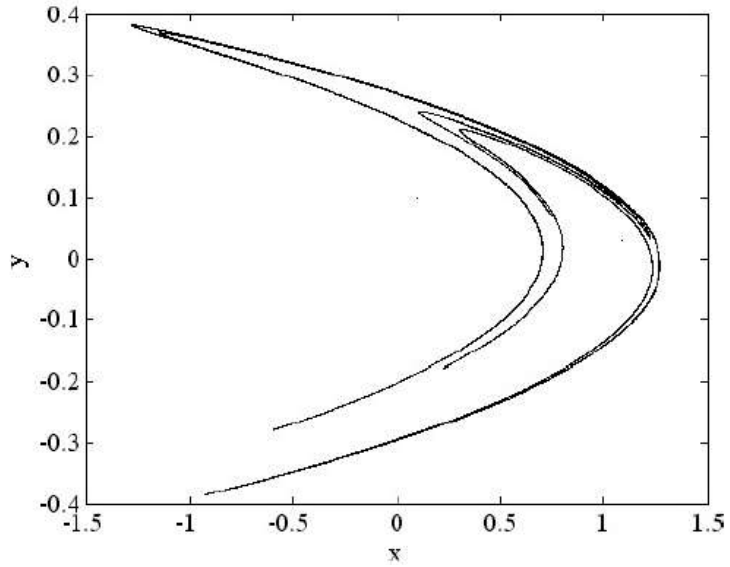

Fig. 3.1 Strange attractor of Henon [5]

Randomness of henon map was tested using Menezes *et al*'s basic tests of randomness, FIPS 140-1 and NIST standard. Results of frequency, serial, poker, runs and auto-correlation were successfully passed when tested against Menezes Test.

The researcher also carried out FIPS 140-1 tests which required 20,000 bits with sequences. five sequences S1 to S5 were generated and passed all tests.

The author also testes the resulted sequence with NIST standard by generating 2×10^8 bits and suit consider it as 200 sequences of 1×10^6 bits each. Threshold for tests was 0.968893 and all tests were within this threshold except variant test. The sequences which even passed Menezes and FIPS 140- 1 tests failed NIST suite tests. For NIST tests choice of parameters to generate bit sequence require attention. such as choosing a large T (about 1000) gives successful results for NIST suite. Resulted pseudorandom bit stream claimed to have good statistical properties when P is large (between 75 to 5000).

Key space size is another aspect which is always looked when analyzing any of the PRNG. For henon map values α , β , X_0 , y_0 and sampling value P together

make the key and key space size for 32 bits and 64 bits sequence the writer found it 97 and 217 respectively.

3.3.2 Chebyshev Polynomial and Tinkerbell Map

In [6] Borislav Stoyanov combined Chebyshev Polynomial and Tinkerbell Map (a type of chaotic map) to generate pseudorandom numbers.

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \qquad \text{Chebyshev Polynomial}$$

$$y_{m+1} = y^2_m - z^2_m + ay_m + bz_m$$
$$z_{m+1} = 2y_mz_m + cy_m + dz_m \qquad \text{Tinkerbell Map}$$

Where a = 0.9, b = - 0.6013, c = 2.0 and d = 0.50.

Initial values of x0 and k of Chebyshev equation and x0 and y0 of Tinkerbell Map are determined with bit stream length L. Both Chebyshev and Tinkerbell are iterated L1 and L2 times respectively, two decimal fractions for xn and ym are obtained to get bitstreams Si and Sj by taking mod 2. Both Si and Sj are XORed to get single bit Sk and this process before XORing is repeated till the time L bit stream is obtained with initial conditions;

x0 = - 0.16029381194009314, k = 2.89, y0 = -0.645622309652631,
z0 = - 0.742799703451115, L1 = 100, and L2 = 200.

Analysis of the proposed scheme was done by using NIST, DIEHARD and ENT tests. For NIST test 1000000 bits consisting of 1000 sequences were generated and all results for these bits were passed and p-value for entropy was 0.446556.

3.3.3 Quantum Logistic Map

In 2014 Akhshani et al generated PRNs using quantum logistic map which was presented by Goggin et al in 1940 [7]. Many researchers worked on introduction of noise into quantum systems including dissipation. to study the effects of

correlation more precisely the quantum correlation on a dissipative system, Goggin et al started with Hamiltonian of kicked quantum system (related to kicked rotors which are prototype models for quantum chaos) coupled to a bath. The system is defined by following equations.

$$x_{n+1} = r(x_n - |x_n|2) - ry_n$$
$$y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r[(2 - x_n - x_n^*)y_n - x_n z_n^* - x_n^* z_n]$$
$$z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r[2(1 - x_n^*)z_n - 2x_n y_n - x_n]$$

where x = <a> (where (a) is annihilation operator), the effects of quantum correction were introduced by a = <a> + δa where δa is quantum fluctuation by <a>. y = < $\delta a^\dagger$ δa> and z = < δa δa> where $a^\dagger$ is boson creation. the β is dissipation parameter and x * and z* are complex conjugates of x and z. Range of r is between 0 – 4 and β selected from 6 - ∞.

To check the **degree of non-periodicity** Akhshani et al use scale index as it is known that for highly non – periodic signal this index will be closer to 1. And observed that when r = 3.99 and $\beta \geq 6$ the scale index becomes max almost = 0.7 and with these parameters the state is highly non – periodic and can be used to generate pseudorandom numbers using quantum chaotic map. While scale index for Henon map was 0.51.

For quantum map Akhshani et al used different **randomness testing suites** including NIST, DIEHARD, ENT and TestU01. As entropy represents the amount of randomness in the sequence and for quantum map its p-value is 0.350485.

To determine the **key space** of quantum map, bifurcation diagram is used with parameters as:

x = 0.62352345, y = 0.0152345, z = 0.0352345, r = 3.99 and β = 10

For robust keys the filled region of bifurcation diagram after 4th periodic window is best suited as it does not contain periodic windows as shown if Fig. 3.2 and key space is 2^{236} which is secure against brute force attack.

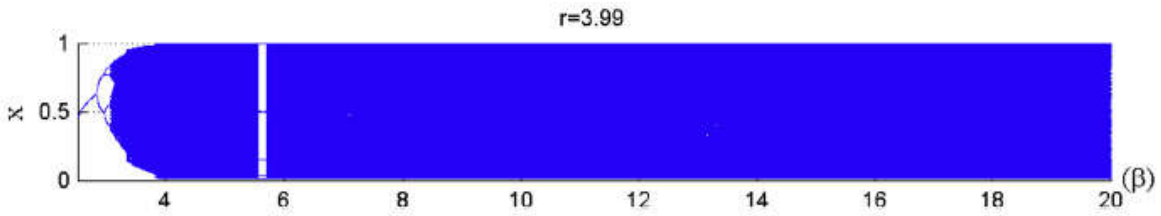

Fig 3.2. Bifurcation diagram for quantum map [7]

The authors also proved that their proposed algorithm is **highly resistive to differential attack** and ideal value for SAD is 2/3 (0.6667) and resulted value is 1/3 (0.33334) and highly resistive to differential attack.

As far as **analysis of speed** of algorithm is concerned the mean speed proved to be 837.05 Mbits/sec on Intel Core i5 – 2467 M CPU at 1.6 GHz with 4GB running on Microsoft windows 8 professional using Microsoft C++ ultimate compiler. Proposed algorithm is fast as number of multiplications in algorithm per byte are 5 and cycles required for each random number generated are 180.

3.3.4 Chaotic Map using Linear Feedback Register

In [8] Ana Cristina DASCALESCU et al. proposed a new discrete chaotic dynamical system to generate PRNG using linear feedback register to address the issues like predictability and choice of improper or limited range of control parameters. Defined Chaotic model was as following:

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

$$f(x) = \arccos\,(\sin(rx) + r^2\cos(rx)) \,/\, 1 + r^2$$

To investigate the **dynamic behavior** of proposed chaotic system, Lyapunov exponent, fractal structure and bifurcation diagram was used. Lyapunov exponent for the proposed scheme, indicating is positive exponent in the map starting from $r \geq 5.5$, hence showing chaotic behavior.

While doing the analysis of proposed scheme before doing randomness test, they discussed **the key space** and claimed as $2^{2144} \approx 2.56 \times 10^{645}$. The key consists of 33 real numbers as initial value and 32 control parameters, and an unsigned

integer. Some **statistical tests** showed that **mean value** appeared to be 127.4688 (almost equal to ideal value of 128), and high values of **standard deviation** (73.9037) and **variance** (5461.8) shows wide spread of bytes over the complete range {0, 1,.., 255}. **Entropy** is also ideal (7.9998), while the **skewness** (-0.0000961) close to zero shows symmetric distribution of values over the mean. **Excess Kurtosis** is used to determine the peak behavior, in this map the negative value (-1.2003) shows flatter peak around the mean.

For **randomness** NIST suite was used and entropy was measured as 0.863690. Proposed algorithm was implemented in C language and run on windows 8.1 using Intel core i3 @2.53 GHz CPU speed with 4 GB RAM and **speed** was 29.12 MB/sec which is very low as compared to quantum map as discussed previously.

3.3.5 Billiard Map

Khalid Sharif et al proposed a new type of PRNG using billiard map which is also a form of chaotic systems [9]. Billiard map is also known as Sinai Billiard as developed by Sinai in 1970. In billiards where a particle moves with constant velocity and hits the border of billiard, reflected particle has same reflected angle as incident angle according to law. These angles and positions of particle are used by the authors as random variables to generate a new PRNG. They took two particles moving in Sinai Billiard and calculated their angles as $I_{0,1}$ and $I_{0,2.}$

These ($I_{0,1}$ and $I_{0,2}$) are used to generate output bit of PRNG as $S_i = I_{i,1} \oplus I_{i,2}$ and S output of PRNG is concatenation of all sub bits (S1,S2, …..). According to researchers to calculate initial angles or conditions 128 bits are required which are taken from password Pw through a pointer, hence 128 bits are enough to define **Key Space** to guard against the exhaustive search attack. They also calculated Hamming distance of key and turned out to be 0.5 which is ideal and shows small change in initial condition will have greater effect overall. For **Randomness** they used NIST standard and all results were successful with entropy 0.851383.

3.4 PRNGs other than Chaotic Maps

There are several other PRNGs which are either based on any cryptographic primitive or has other design structures not based upon chaotic maps. Although there are different chaotic maps other than discussed in section 3.3 which are used for PRNGs or with same chaotic map implementation method is improvised to generate maximum sequence in less time with randomness properties, like in [38] researchers utilized S-Box with logistic map to increase the entropy (0.74287) and 15852 bits per second as max speed. Xoroshiro 128+ is latest proposed PRNG and considered to be the speediest PRNG with low memory (128 bits).

Type of Generator	**Year of Publish**	**Underlying Hard Problem**	**Period**	**Key Bits n**	**Speed**
Xoroshiro 128+	2016	Improvised Xorshift	2^n -1	128	1.2 nanosec / 64 bit number
Xorshift	2003	Linear feedback Shift Register	2^n - 1	64 & 128	1 billion numbers in 32 secs
Well equidistributed Long – period Linear (WELL)	2006	Linear recurrences mod 2	2^n - 1	512,607, 800, 1024……44 497	10^9 numbers in 35.8 secs for 512
RC4	1987	RSA	2^n - 1	40 - 2048	7 cycles per byte
Park – Miller Random number generator	1988 2009(chan)	Linear congruential generator	2^n - 1	31	
Multiply – with – carry	1991	Arithmetic Mod	2^{60} to $2^{2000000}$	15 – 512	
Mersenne Twister	1997	Linear Feedback Shift register 32 bits	$2^{19937}-1$	19937	4.7 ms for 5×10^7 random 32-bit integers
Yarrow	2012	Hash Function and Triple DES		160 bits	
Blum Blum Shub	1992	Prime Factorisation		92 bits	
ISAAC	1993	Steam Cipher		2466	
Lagged Fibonacci generators	2009	LCG (Fibonacci Sequence)	$(2^k - 1)*2^{M-3}$ $2^{2300000}$		

Table 3.1 Different Pseudorandom Generators other than Chaos Based

3.5 Conclusion

A lot of work has been done in Chaotic Pseudorandom Number Generation and different maps are suggested by the researcher for PRNG. Researchers have also used latest tools to identify the robustness and security of the proposed schemes. As entropy gives the uncertainty of outcome and for randomness this should be high. Although Billiard map and chaotic map using Linear feedback shift register give high entropy rates as compared to Quantum map and Chebyshev map but, earlier are continuous chaotic maps which are efficient but not secure against algebraic attacks as compared to discrete chaotic maps. As compared to PRNGs designed other than chaotic maps are having long period and efficient bit generation rate, however if chaotic maps are also based on same design like in section 3.3.4 chaotic map is proposed using linear feedback shift register with high entropy rate and having key space 2^{2144} generating 29 Mbits/sec then effective length of sequences can be generated in efficient manner.

Chapter 4

Framework for Analysis of Chaotic Maps

4.1 Introduction

Over the period researchers worked for finding the best tests for analysis of pseudorandom numbers, generated through different algorithms. Some of these were discussed in the previous chapter and NIST standard SP800-22 has been developed for checking the randomness with 15 different tests. However, as far as chaotic random number generators are concerned before testing the randomness of the numbers generated, it is more important to find the perfect initial conditions from where a chaotic map enters the chaotic region.

In this chapter we will see what properties or tests define the chaotic region and how they are determined. Although these tests never been included in any testing standard, but the proposed chaotic random number generators have been using these tests to verify the initial conditions to increase the efficiency of the functions. Analysis includes Lyapunov Exponent, bifurcation diagram and phase diagrams.

4.2 Chaotic Region Determination [11]

4.2.1 Lyapunov Exponent

A logistic map exhibits aperiodic orbit, but when this map enters chaotic region that is required to be determined. A chaotic map is always sensitive to initial conditions and dependence to initial condition is defined by Lyapunov exponent as LE shows three properties i.e; stable, periodic and chaotic. Sensitive dependence is quantified by defining the Lyapunov exponent for a chaotic map, hence it can be said that LE is quantitative measure of chaos in a system. Let's consider a one-dimensional chaotic equation with initial condition x_0 and having nearby point as $x_0 + \delta_0$. δ_n be the separation after n iterations. if $| \delta_n | = | \delta_0 | e^{n\lambda}$ then λ is called Lyapunov exponent. λ will be positive for chaotic maps and and negative for fixed points and cycles. It can also be defined as following:

$$\lambda(x_0) = Lim\ N \rightarrow \infty\ (1/N \sum_{n=1}^{N} ln\ |f'(x_n)|$$

Like in the feedback shift register chaotic mapping the Lyapunov exponent is plotted as shown in Fig. 4.1, where it can be seen when r≥ 5.5 it enters chaotic region.

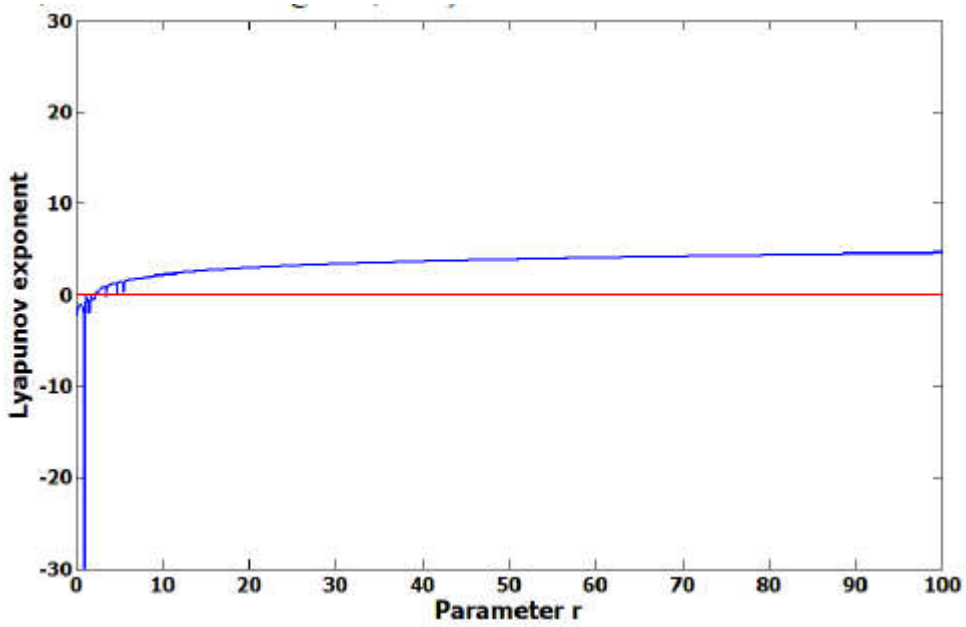

Fig. 4.1 Lyapunov Exponent [8]

4.2.2 Bifurcation Diagram

As we see LE gives us quantitative measure of chaos while the bifurcation diagram is qualitative measure or analysis of chaotic systems, since qualitative changes in dynamics is known as bifurcation. Chaotic systems are sensitive to initial conditions, so the initial conditions or parameters bring changes to the system and known as bifurcation points.

Saddle – Node Bifurcation. This is the fundamental type of bifurcation, which deals with the creation and destruction of fixed points. With the change in parameters two fixed points (stable and unstable) move towards each other and mutually annihilate after collision. Let's consider as system with following equation: $x' = r + x^2$

It generates three different graphs depending upon the value of *r (*positive, negative or zero), as shown in Fig 4.2.

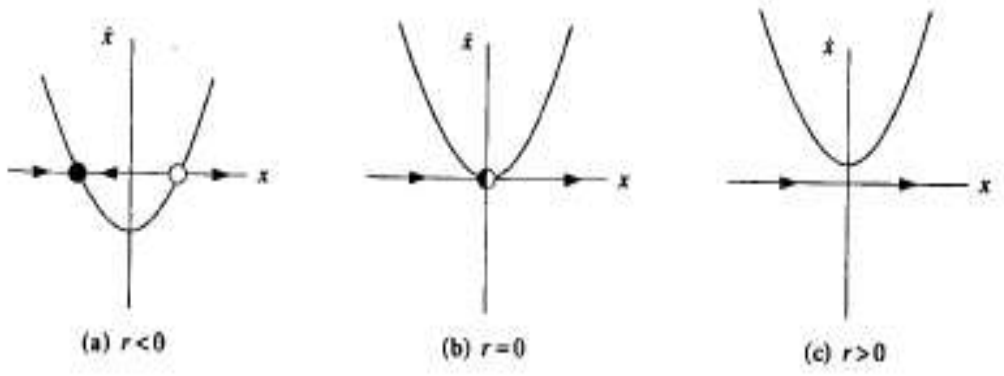

Fig 4.2 Saddle Node Bifurcation [11]

when r < 0 and approaches 0 from below the two fixed points move towards each other (Fig 4.2a) and when r = 0 then two points coalesce each other and becomes half stable fixed point at x' = 0 (Fig 4.2b). When r>0 the fixed point vanishes and there are no fixed points now, so bifurcation occurred at r = 0.

Transcritical Bifurcation. There are some systems in which fixed points should exist and never vanished for all values of parameter or initial conditions, such as Logistic equation. The stability of fixed points may vary with change in parameters. transcritical bifurcation is known as standard method for such stability changes. Normal form of transcritical bifurcation is given by equation:

$$x' = rx - x^2$$

It is like a logistic equation allowing x and r to be positive and negative both, giving plot as Fig 4.3 depending upon the value of r.

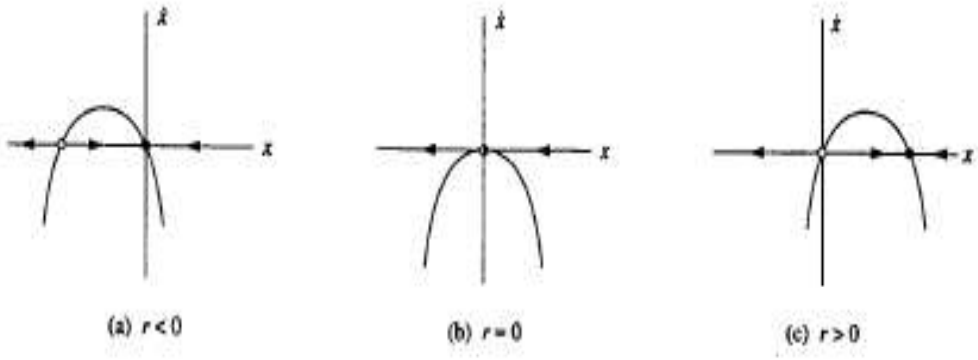

Fig 4.3 Transcritical Bifurcation [11]

It can be seen in the Fig 4.3 above that for all values of r there exists fixed point at x' = 0. There is unstable fixed point when r<0 at x' = r and when value of r increases the unstable point moves towards origin when r = 0. when r>0 the origin becomes unstable and the point at x' = r becomes stable. This phenomenon is also known as exchange of stabilities.

So, with these two forms we can conclude that in saddle node point the fixed point is destroyed while in transcritical bifurcation the point never disappears after bifurcation, but switches stabilities. There is also another form of bifurcation known as pitchfork bifurcation used for physical problems having symmetry. This bifurcation is for one dimensional system when we shift to 2D then saddle- node point bifurcation exhibits a ghost after annihilation which effects afterwards also. Fig 4.4 describes same behavior for the equation:

$$x' = \mu - x^2$$
$$y' = -y$$

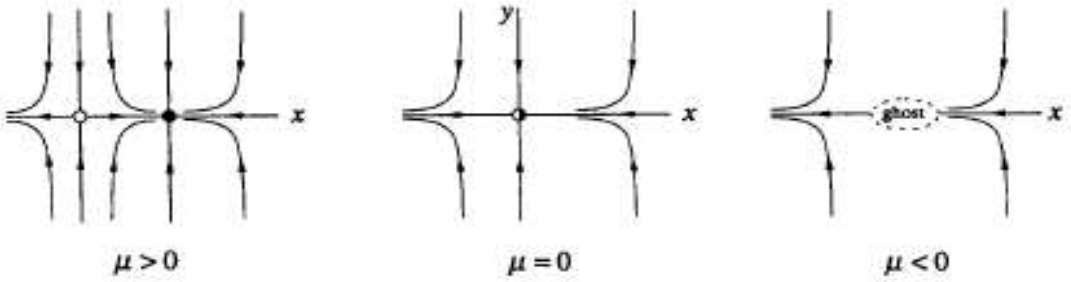

Fig. 4.4 Pitchfork Bifurcation [11]

Bifurcation diagram for the simple Lorenz Equation is given by Fig 4.5.

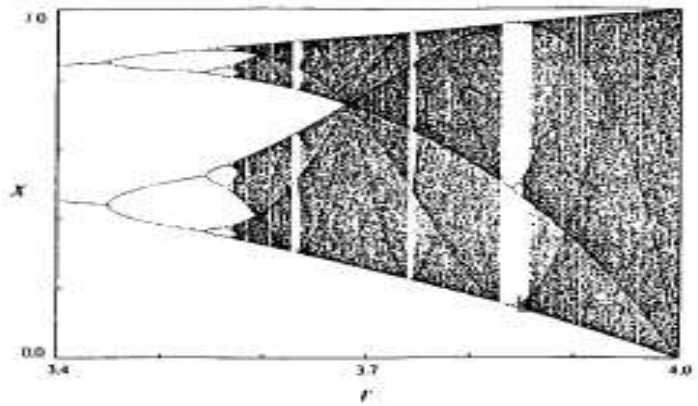

Fig. 4.5 Bifurcation Diagram [11]

From Fig 4.5 qualitative measures are achieved showing best values for parameter r. It is also visible that there exist periodic windows in the plot for $r > r_\infty$. At r = 3.8284 the third periodic window starts, which is the basically saddle node bifurcation and known as tangent bifurcation and fixed points are annihilated but still presence of ghost is there. But as we move down to chaotic region the hills and valleys move down and up ad curve is pulled away from diagonal. So, through bifurcation diagram we find quality of chaotic region.

4.3 Improvised Chaotic Map to Enhance Properties

We have seen analysis of Chaotic maps both quantitatively and qualitatively, but still there is choice of algorithm which enhances the properties of these maps. Such map was discussed by Machicao and Bruno in [10] and named as k – logistic map. Let's consider a logistic map with equation $x_{t+1} = f(x) = \mu x_t(1 - x_t)$, where $\mu \in [0,4], x \in [0,1]$ and t is discrete time step. Fig.3.6 shows the time evolution of k - logistic map having t = 100 iterations with orbits from k_0 to k_4. Lyapunov exponent shows three stability behaviors as chaotic, periodic and stable.

In Fig. 4.6(a) $\mu = 4$, Fig. 4.6(b) $\mu = 3.75$ and Fig. 4.6(c) $\mu = 2.85$

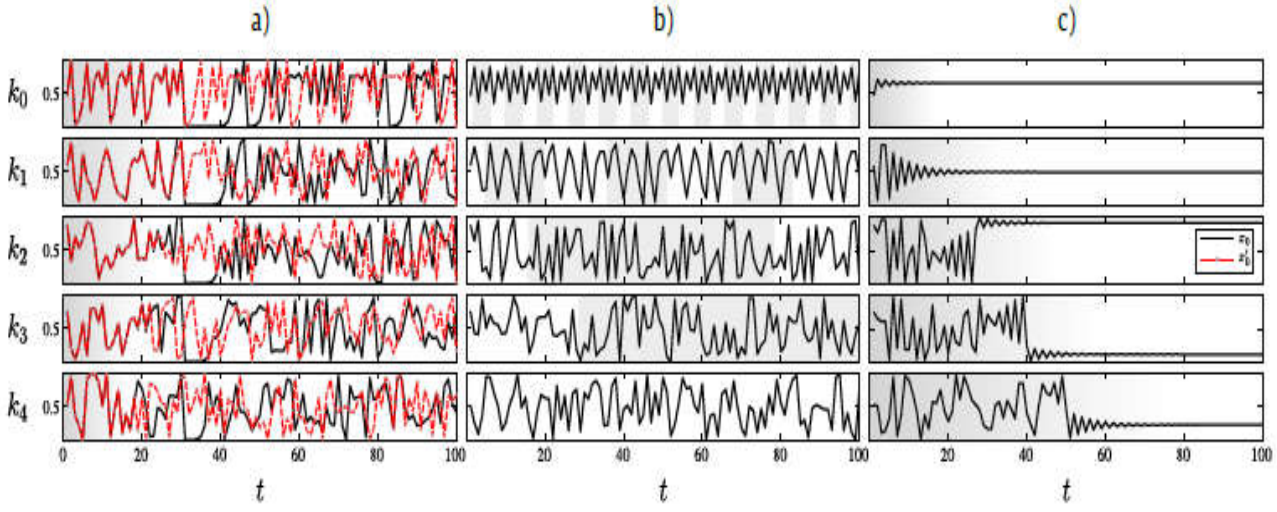

Figure 4.6. Time-evolution of two orbits with close initial conditions $x_0 = 0.4587525281$ (solid line) and $x'_0 = 0.4587525282$ (dotted line) [10]

They defined a length of decimals to be picked for algorithm as L and further defined a k value for the decimal values to be left after decimal point and to make the length as equal to L rest of the sequence is padded with 0. So k_0 means no figure will be left after decimal point and k_4 means value after decimal point will be picked after three figures; if x = 0.457525281 then it is also equal to k_0 but having L = 6 means it will be 0.457525 where as k_4 will be 0.525281 for L = 6. So, making algorithm flexible and having choice of value as moving from k0 to k4 it can be seen from figure 4a that number of iterations are reduced where two different values diverge from 31 to 17.

Upon further analysis it revealed with bifurcation diagram Fig 4.7. that zigzag behavior almost vanished at k4 and patterns are more filled as 'k' increases.

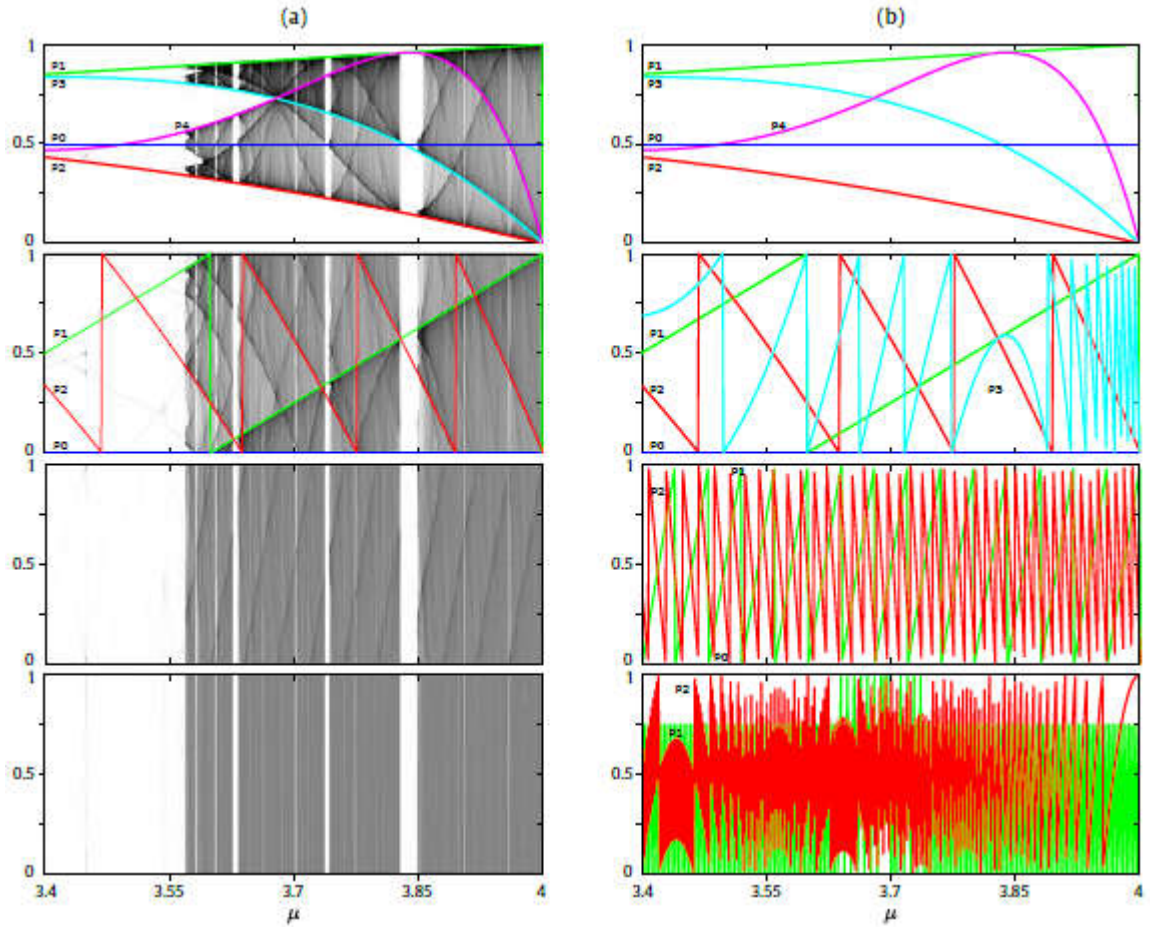

Fig 4.7. Bifurcation Diagram and Zig Zap plot for k – logistic map [10]

Lyapunov exponent for same also shows that chaotic region value for k1, k2, k3 and k4 are well above k0. Fig 4.8.

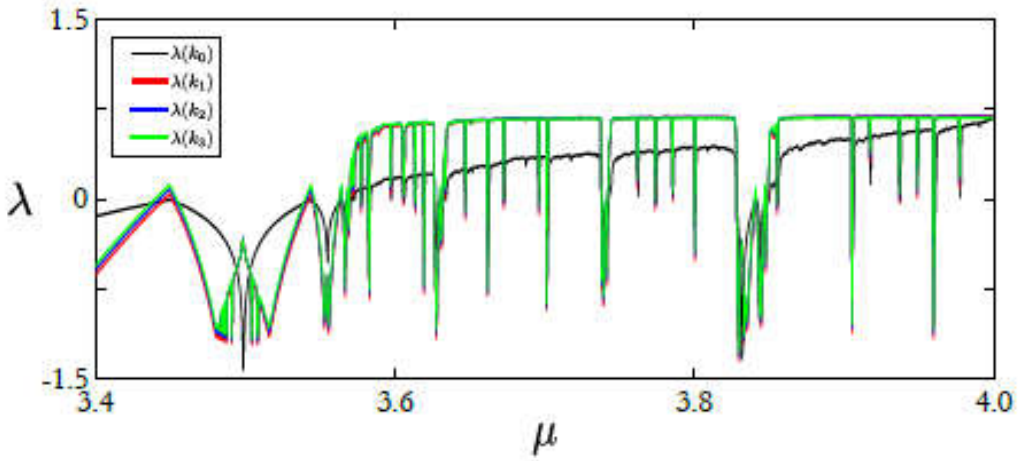

Fig 4.8. Lyapunov Exponent plot for k – logistic map [10]

4.4 Conclusion

After defining the framework to analyze the chaotic maps quantitatively and qualitatively chaos can be defined as " a long term aperiodic behavior", because there are trajectories which do not settle to a fixed point, periodic orbit, or bits as t→ ∞, and it is also "deterministic", because the system does not have any random or noisy inputs or parameters, and "sensitive to initial conditions", since nearby trajectories diverge exponentially very fast having positive LE. It also gives choice of algorithm for implementation giving major advantage over other PRNGs having one fixed algorithm with defined period.

Chapter 5

Cryptographic Properties of Chaotic Maps

5.1 Introduction

Although Chaotic based cryptography gives advantage of ergodicity, sensitive to initial conditions and choice of algorithms too, but as per Kirchhoff's principle the security of any algorithm is basically the key and it does not depend on the hidden schemes or algorithms. These maps are iterative and give property of rounds as in symmetric encryption but result in slow speed. Hence for analysis of cryptographic properties of these chaotic maps these two features; i.e. speed and key space, must be determined. In chapter 2 many chaotic maps are discussed with their speed and key space and chapter 3 describes the framework for analysis of these maps and variation in implementation one can have by varying the decimal places. In this chapter the focus will be to analyze the cryptographic properties (speed and key space) of chaotic maps using same framework and methods discussed in earlier chapters to generate a random sequence using chaotic maps.

5.2 Speed of Chaotic Maps

Chaotic maps are iterative functions to generate desired sequence having randomness. These iterations make the algorithm slow, especially when using floating point numbers. Arithmetic operations on floating point has always been time consuming and expensive as a 64-bit processor uses 6 times more clocks as compared to same operation on integers [12]. IEEE 754 defines arithmetic formats, interchange formats, rounding rules, operations and exception handling for processors and was revised in July 2019 as IEEE 754-2019 [13]. According to these rules number representation cannot be infinite and there are rules for rounding off the decimal points. Since chaotic maps are sensitive to initial condition hence small change in number representation and rounding off rules makes huge change in results. In [14] Pisarchik et al showed when mean squared error computed on two different processors, using logistic map as in Fig 5.1. After 30 iterations there is nothing common in both calculations. Any message longer than 30 bits which is very less in practical will not be decrypted at other end. However, if at all the processors produce same sequence then different software implementation would result into different floating-point number representation. Hence to implement chaotic crypto

systems identical implementation engines are required at both ends, which reduces flexibility of implementation.

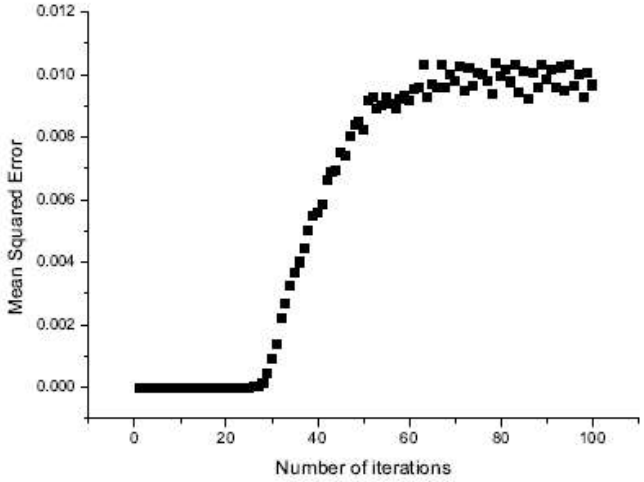

Fig 5.1 Mean Squared Error between two 32 - bit different processors [14]

5.3 Key Space

For n – bit crypto scheme we can have 2^n keys with period $2^n - 1$. But as we have seen earlier chaotic maps exhibits periodic windows, due to which this formula is not applicable to it. For calculating the key space of chaotic maps, formula being used is known as Shannon seminal formula and defined as:

$$D_{ks} = log_2 (N_v - 1.5\ N_{pw})$$

Where N_v are the number of points within in chaotic region and N_{pw} are points in periodic windows which is multiplied by security factor 1.5. In [14] the researcher calculated key space of logistic map while varying the decimal points of value of x by number of digits 5, 6, 7, and 8, using chaotic region between 3.57 – 4 and key space came out to be 15, 18, 21 and 25 bits respectively.

But on analysis of logistic map, it shows that there exist periodic windows in between 3.57 and 4. It can be analyzed if both Lyapunov and Bifurcation diagrams are mapped together as in Fig 5.2. There are three periodic windows and largest one with negative Lyapunov exponent is in between 3.83 and 3.85.

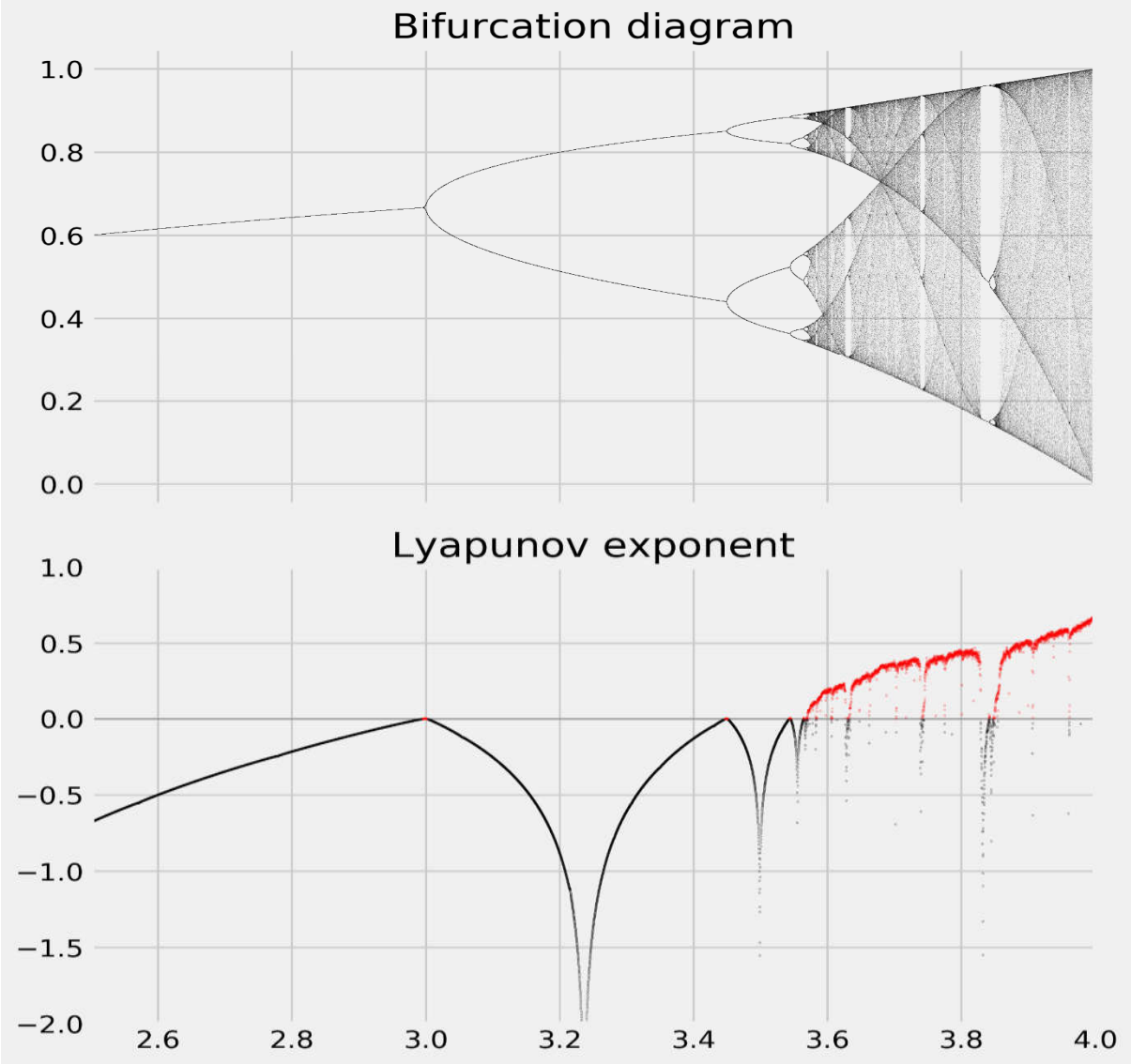

Fig. 5.2 Lyapunov and Bifurcation Diagrams of Logistic Map

Although Fig. 5.2 does not give exact values for periodic windows but gives idea of starting and ending region. In order to find the exact values, there is method of coweb plotting for one dimensional map. A coweb plot showing inward spiral means stable fixed point (Fig. 5.3) for r = 1.5 since abs (2 - r) <1 , while an outward one shows unstable fixed point.

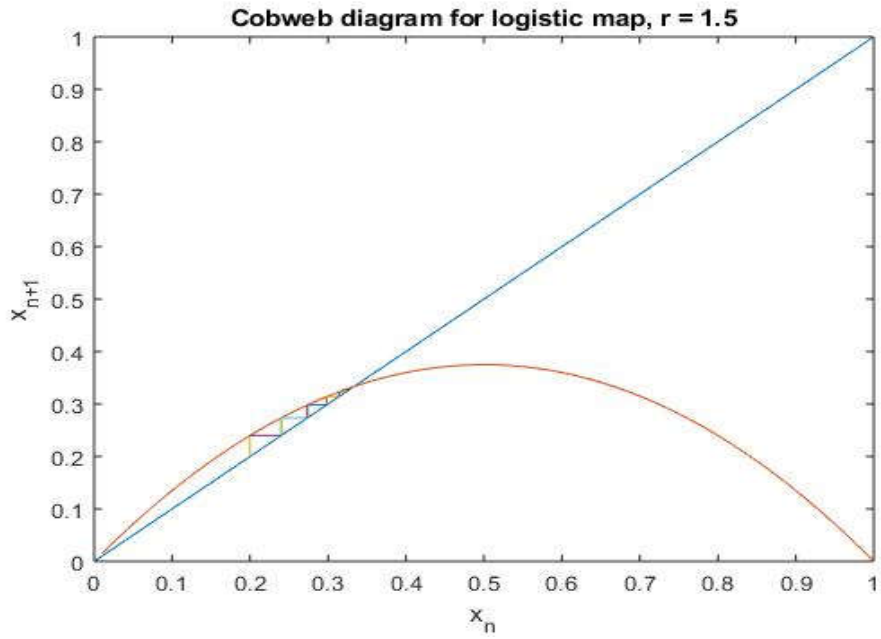

Fig. 5.3 Stable Fixed Point

First period doubling starts at r = 3 and can be seen in Fig. 5.4(a) with rectangle. While a chaotic orbit shows filled out area, having infinite number of non-repeating values as depicted in Fig 5.4 (b).

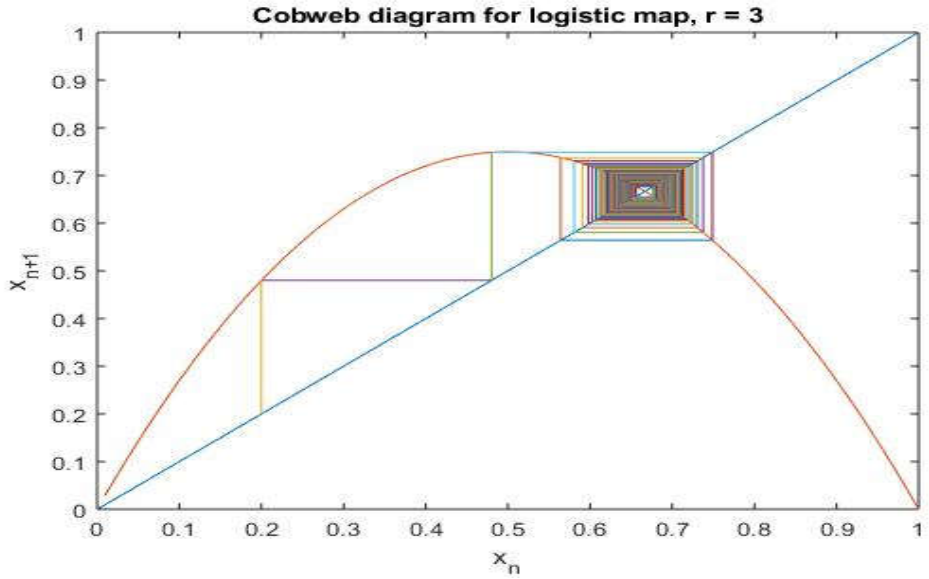

Fig. 5.4a. Period 2 at r = 3

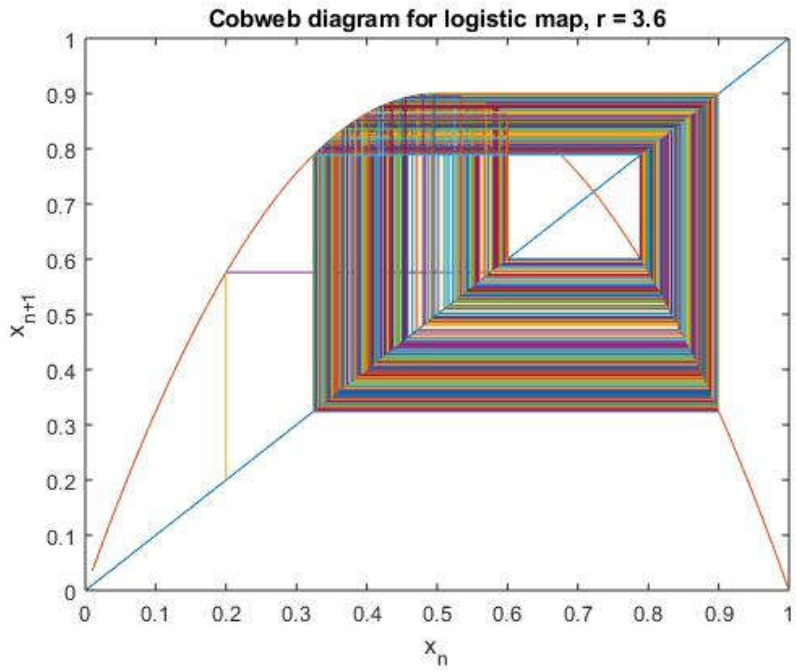

Fig. 5.4b. Chaotic Region for Logistic Map at r = 3.6

After r = 3.57 the periodic window starts at 3.83 as shown in Fig. 5.5(a) and next chaotic region starts at 3.85 Fig. 5.5(b).

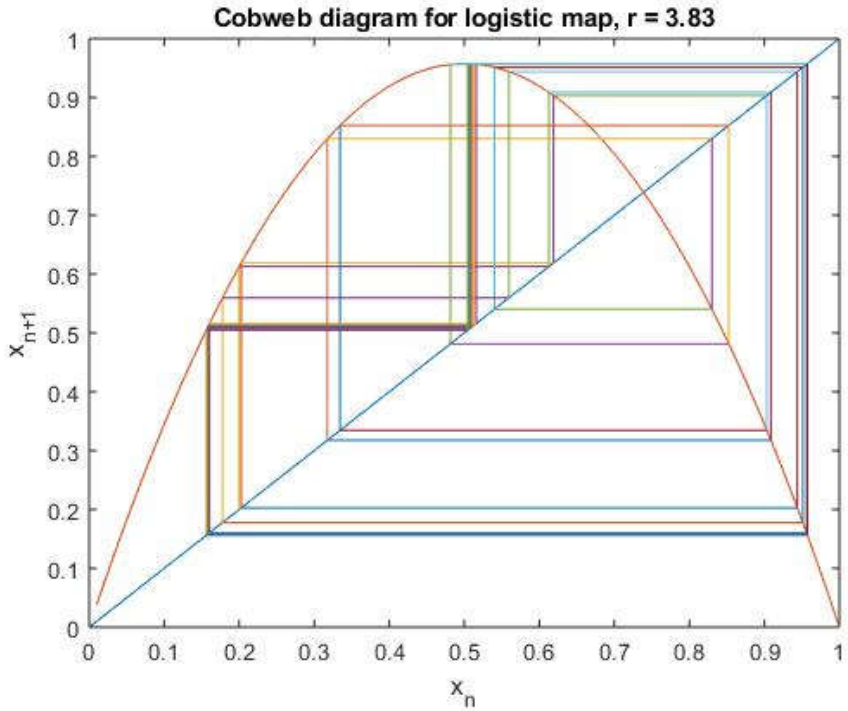

Fig. 5.5a. r = 3.83

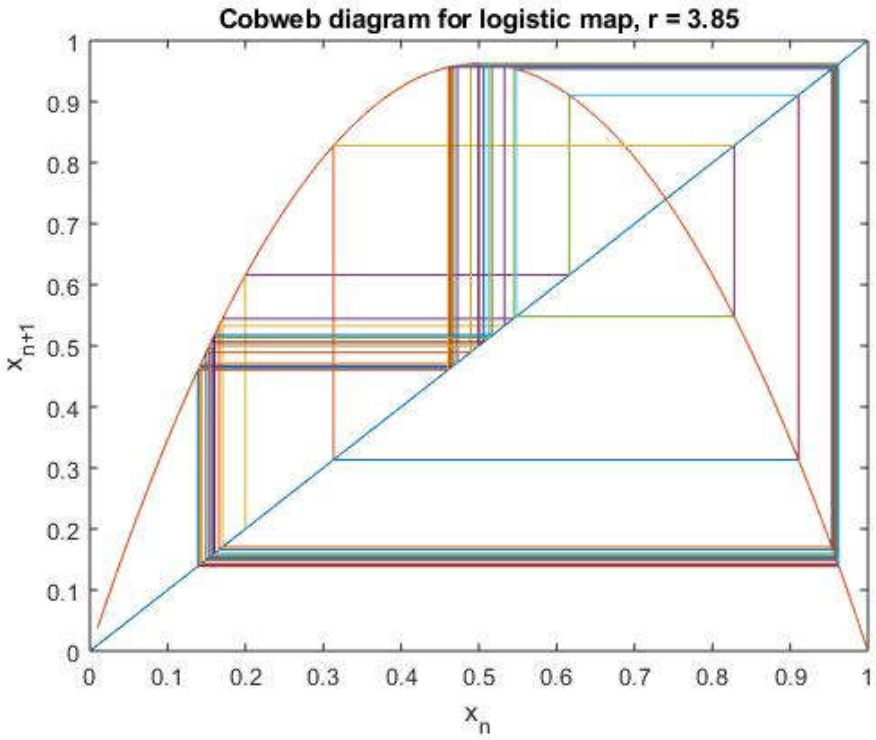

Fig. 5.5b. r = 3.85

Key space for the region (r = 3.57 – 3.83) is calculated using the MATLAB code, by not only varying the decimal points of *x* but also the control parameter *r* using Intel 1.61 GHz 64 – bit processor for chaotic region as 3.57 – 3.83. Results are in Table 5.1.

The results show that after reducing value of r (3.57 – 3.83) there is hardly any difference in number of bits between the values of given in [14] and Table 5.1. Reason for this is that in [14] the effective value of *r* is (3.57 – 3.97) as it is calculated to 1 decimal point of *r* and software calculates it till 3.97. However, with increase in number of decimal points whether in *x* or in *r* the key space increases. But with increase in number of decimal points of *r* the effective utilization of whole region is also increased, resulting in increased key space. But at the same time the calculation time increases with increase in number of decimal points. However at *r* = 4 maximum points are achieved in logistic equation hence if we calculate number points with 5 decimal places of *x* and 1 decimal place of *r* between region 3.9 – 4 then 12042 points are generated giving 13.55 bits key length and with 2 decimal places of *r* it comes out to be 16.38 bits hardly making 1 bit difference for the same number of decimal points as calculated in Table 5.1.

***x*(decimal points)**	***r*(decimal point)**	**Total Points generated**	**Key Bits**	**Time taken (secs)**
5	1(3.77)	30001	14.87	0.55
6	1(3.77)	269921	18.04	0.656
7	1(3.77)	2259900	21.11	2.555
8	1(3.77)	30000001	24	34.646
5	2(3.83)	252031	17.94	0.8
6	2(3.83)	2603731	21.31	3.154
7	2(3.83)	25064462	24.57	22.106
8	2(3.83)	260388999	27.95	1023
5	3(3.83)	2437674	21.21	2.819
6	3(3.83)	24291544	24.5	21.098
7	3(3.83)	247908143	27.8	1284.394

Table 5.1 – Key Space Calculation of Logistic Map By varying decimal places of *x* and *r*

On further analysis of LE diagram with increasing decimal points of r it is very much obvious that the periodic behavior increases with increase in decimal points of r. Like the highly chaotic region of logistic map is considered from 3.9 – 4. If the two decimal places are taken for r then LE diagram appears as in Fig 5.6 with all positive LE values.

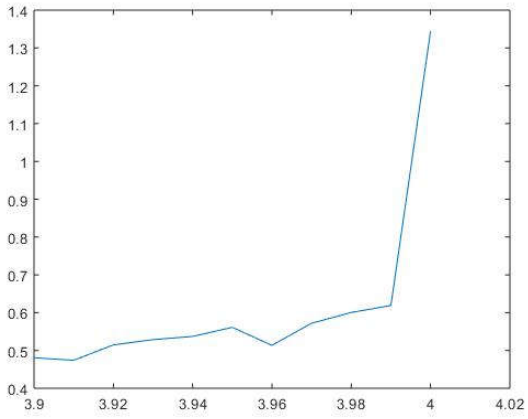

Fig. 5.6 LE Diagram for r = 3.9 to 4 with difference of two decimal places

On increasing the decimal places from 2 to 3 there exists 2 periodic windows giving negative LE values as shown in Fig 5.7.

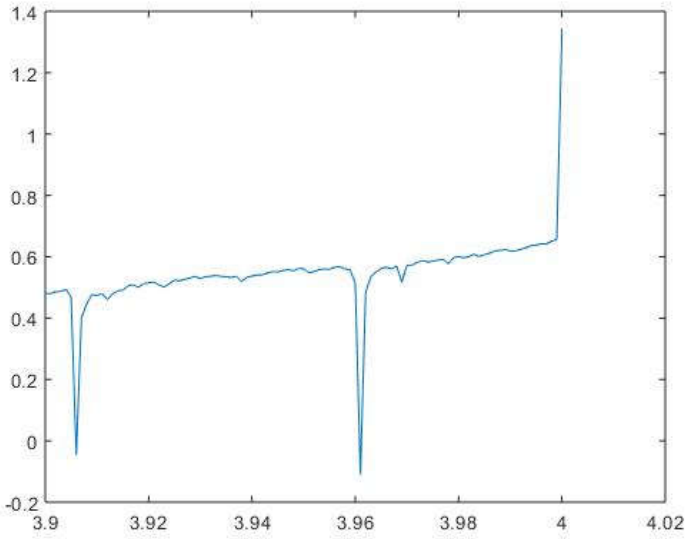

Fig. 5.7 LE Diagram for r = 3.9 to 4 with difference of three decimal places

With increase in decimal places of r the periodic windows increase as for four decimal places the number of negative values of LE increases to 10 (Fig 5.8). Hence it can be deduced that increase in decimal places increases number of points but at same time there are periodic behaviors which can be observed by LE diagram. So, for control parameter 'r' of logistic map the effective value to be varied is up to two decimal places.

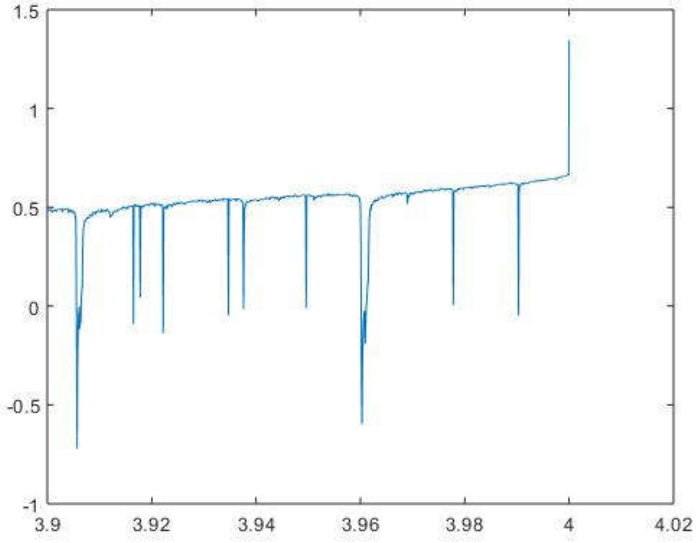

Fig. 5.8 LE Diagram for r = 3.9 to 4 with difference of three decimal places

If whole chaotic region is required to be used for logistic map, then 'r' to be varied with 1 decimal point then LE for whole region remains positive as shown in Fig 5.9

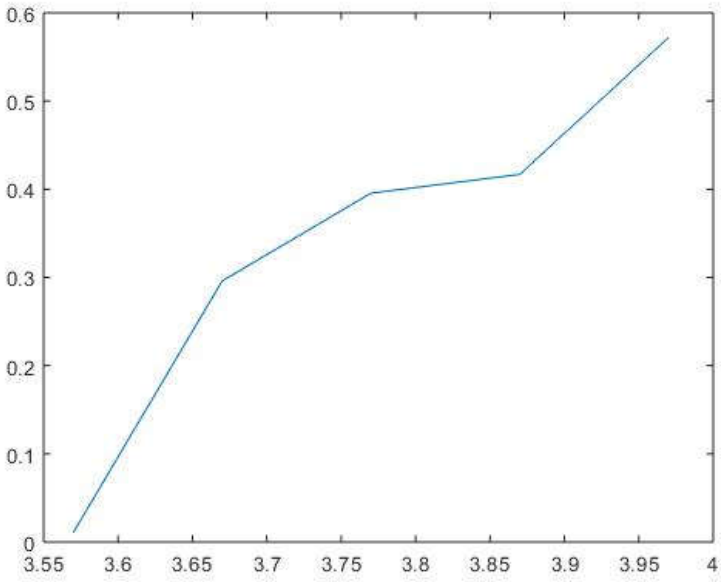

Fig 5.9 For complete chaotic region with r = 3.57 – 4 with 1 decimal place

Another interesting and secured implementation of chaotic map is to use transient value of initial point (x_0) instead of chosen initial value with desired number of iterations. For example, with initial condition x_0 = 0.5 after 500 iterations before generating the desired sequence the value of x_0 becomes 0.7630 when r ranges between 3.9 – 4, and after 100 iterations 0.3236 also changing the key length. After 1000 iterations transient value becomes 0.0701 with a greater number of points (85658 to 85901) for r varying 2 decimal places from 3.9 – 4. So, if at all initial value of x is known to adversary the right sequence cannot be generated till the time number of iterations are unknown and securely communicated between encrypting and decrypting party. So, with same initial condition for different sessions the key can be generated with hidden number of iterations for each session.

5.4 Analysis

Results given in section 5.3 show that key space can be defined for the chaotic region based upon number of variables, the number of control parameters and the number of values it can take. So, for a complete chaotic region of logistic map from 3.9 – 4 there

will be 100 places where different points of x can be calculated. As there is one variable and one control parameter the key space for this region would be 10^2 x 10^2 (i.e; 10000), taking $\log_2(10000)$ comes out to be 13.28 bits. For any cryptographic primitive if chaotic maps are used, for initial key agreement the initial values of variables are transmitted in plaintext, hence it will further reduce the key space as in discussed case it would be 100 resulting into 6.64 bits only. For brute force attack the space becomes narrow and easier for exhaustive search. However, for 1 decimal place of control parameter whole region produces positive LE hence key size will be 10x10 (6.64 bits).

The **orbit length** can be determined by using formula [39] 2^{ε^L} where ε is distance between two neighboring points and $\varepsilon \geq 2^n$ for integers and $\varepsilon = 2^{-n(x)}$ for real numbers [40]. and L is the word size (the precision). Cycle n of any chaotic map is given by $n \leq 2^L$, however if transient value for initial condition is used then and transient length is l then cycle will be $l + n$.

Experimented results for logistic map with different initial conditions and different values of control parameter 'r', generated points with different precision level are tabulated as Table 5.2 for 10,000 iterations. From calculated orbit lengths no, specific formula can be applied for calculating the orbit cycle of any chaotic map. orbit length of any chaotic map depends upon the its construction and structure of function, control parameters and initial conditions with precision level. However, it is fact that with increase in decimal point correction the key space increases as shown in Table. 5.1.

Initial Value of x	Value of r	Precision (decimal place)	Number of points	Orbit Length	Precision (decimal place)	Number of points	Orbit Length
0.1	3.57	1	10,000	Unknown	2	10,000	Unknown
0.2	3.57	1	10,000	Unknown	2	10,000	Unknown
0.3	3.57	1	8	8	2	10,000	Unknown
0.4	3.57	1	2	2	2	10,000	Unknown
0.5	3.57	1	4	4	2	32	32
0.6	3.57	1	10	10	2	10,000	Unknown
0.7	3.57	1	1	1	2	10,000	Unknown
0.8	3.57	1	2	2	2	12	12
0.9	3.57	1	4	4	2	22	22
0.1	3.57	3	10,000	Unknown	4	10,000	Unknown
0.2	3.57	3	10,000	Unknown	4	10,000	Unknown
0.3	3.57	3	10,000	Unknown	4	10,000	Unknown

0.4	3.57	3	10,000	Unknown	4	10,000	Unknown
0.5	3.57	3	224	224	4	5536	5536
0.6	3.57	3	10,000	Unknown	4	10,000	Unknown
0.7	3.57	3	10,000	Unknown	4	10,000	Unknown
0.8	3.57	3	10,000	Unknown	4	10,000	Unknown
0.9	3.57	3	10,000	Unknown	4	10,000	Unknown
0.1	3.67	1	10,000	Unknown	2	10,000	Unknown
0.2	3.67	1	6	6	2	10,000	Unknown
0.3	3.67	1	6	6	2	26	26
0.4	3.67	1	2	2	2	18	18
0.5	3.67	1	18	18	2	38	38
0.6	3.67	1	14	14	2	16	16
0.7	3.67	1	1	1	2	100	100
0.8	3.67	1	2	2	2	28	28
0.9	3.67	1	2	2	2	4	4
0.1	3.67	3	10,000	Unknown	4	10,000	Unknown
0.2	3.67	3	10,000	Unknown	4	10,000	Unknown
0.3	3.67	3	52	52	4	2960	2960
0.4	3.67	3	132	132	4	2600	2600
0.5	3.67	3	162	162	4	6988	5536
0.6	3.67	3	357	357	4	4412	4412
0.7	3.67	3	126	126	4	4156	4156
0.8	3.67	3	478	478	4	2384	2384
0.9	3.67	3	22	22	4	322	322
0.1	3.78	1	2	2	2	10,000	Unknown
0.2	3.78	1	8	8	2	2	2
0.3	3.78	1	4	4	2	8	8
0.4	3.78	1	2	2	2	35	35
0.5	3.78	1	2	2	2	28	28
0.6	3.78	1	4	4	2	54	54
0.7	3.78	1	1	1	2	24	24
0.8	3.78	1	4	4	2	160	160
0.9	3.78	1	2	2	2	7	7
0.1	3.78	3	10,000	Unknown	4	10,000	Unknown
0.2	3.78	3	278	278	4	539	539
0.3	3.78	3	570	570	4	8224	8224
0.4	3.78	3	1566	1566	4	4374	4374
0.5	3.78	3	605	605	4	7399	7399
0.6	3.78	3	54	54	4	769	769
0.7	3.78	3	823	823	4	823	823
0.8	3.78	3	357	357	4	1665	1665
0.9	3.78	3	92	92	4	1511	1511
0.1	3.97	1	7	7	2	11	11
0.2	3.97	1	3	3	2	103	103

0.3	3.97	1	5	5	2	13	13
0.4	3.97	1	6	6	2	15	15
0.5	3.97	1	4	4	2	108	108
0.6	3.97	1	3	3	2	50	50
0.7	3.97	1	6	6	2	241	241
0.8	3.97	1	4	4	2	22	22
0.9	3.97	1	2	2	2	13	13
0.1	3.97	3	587	587	4	588	588
0.2	3.97	3	445	445	4	550	550
0.3	3.97	3	775	775	4	1175	1175
0.4	3.97	3	753	753	4	1261	1261
0.5	3.97	3	268	268	4	4470	4470
0.6	3.97	3	50	50	4	1700	1700
0.7	3.97	3	358	358	4	6685	6685
0.8	3.97	3	599	599	4	10,000	Unknown
0.9	3.97	3	662	662	4	5840	5840

Table 5.2 Different Cycles for Logistic Maps

Other aspect which effects entropy and ultimately randomness of bit sequence is algorithm for generating bits stream from generated real numbers. For calculating bits stream two methods are applied for generating 10,000 random numbers with initial condition of x = 0.1 with precision upto 5 decimal places for chaotic region of logistic map (3.57 – 4) with step of 0.1. Total outputs generated are 421,028 and first 10,000 numbers were picked for random number generation.

Method1. The output value is compared with a threshold value set to 0.5.

if $x_{n+1} > 0.5$ then output bit is 1

if $x_{n+1} < 0.5$ then output bit is 0

The output stream was stored in .txt file and approx. entropy calculated using NIST suite for randomness tester by taking block size '8' recommended by NIST tool ($\log_2 n$) where n is length of bits stream (10,000). Calculated Approx. Entropy for this method is 0.1141 and total time for calculation of generated sequence including bit conversion is 0.504 secs.

Method2. The output value is converted to integer for first decimal place and then by taking mod 2 the bit decided either to be 0 or 1 .

Entropy for this method is 0.0604 and total time for calculation of generated sequence including bit conversion is 479 secs ≈ 8 mins.

From results of both methods it is obvious that selection of algorithm for generating bit stream also has effect on speed and randomness, so balance in between should be maintained for effective randomness and robustness.

There are many advantages of chaos-based cryptography and certain limitations too which are discussed as under:

5.4.1 Advantages of Chaos-Based Cryptography

Chaos based cryptography has many advantages over traditional cryptography, which are discussed in this section as per given analysis.

There are many types of chaotic functions with different key space. The developers can use these functions for different cryptographic purposes as per key space available. These purposes could be generation of nonce (using chaotic maps with small key space), creation of cryptographic keys with chaotic maps having more than 128 bits key space.

Another advantage which these maps provide is choice of algorithm which can be used for creation of random numbers based upon the selection of decimal points for initial conditions of variables and criteria for bit generation. As many image encryption schemes use number of pixels as modulus value to convert the decimal points into integers and then the binary representation of these integers is XORed with images to encrypt the image. In symmetric encryption the easiest way to generate sequence from these decimal values is to compare current number with previous number and decide bit value as 1 or 0 based upon greater or smaller. There are certain algorithms which use a threshold value to generate the bit sequence also. Improvised chaotic map discussed in section 4.3 is one of the examples for choice of algorithm and discussed methods in analysis part are two examples how entropy changes with change in algorithm.

The chaotic maps mostly used are Iterative in nature. In block ciphers different number of rounds are used for key scheduling. Hence, if these maps used in

symmetric encryption can provide characteristics of rounds for key scheduling being iterative in nature.

Ergodicity is main property of chaotic maps, which means for any input the output has same distribution, this is same as confusion in cryptographic schemes.

Chaotic maps also exhibit property of diffusion as they are sensitive to initial conditions and minor change in initial values results in different outputs. Section 4.3 Fig 4.6(a) shows the same results for two different values of x, as x_0 = 0.4587525281 and x'_0 = 0.4587525282.

Pseudorandom generator's security lies with its secure initial conditions. In chaotic maps it is achieved through generating transient value through different number of iterations, if at all attacker gets the initial value at receiver or transmitter end, however she cannot generate the right sequence till the time she can get that transient value. This transient value also increases the entropy of the pseudorandom number generator.

Different chaotic maps can also be grouped together for high dimensional maps to increase the key space. Like 1D logistic map can be grouped with 2D henon map to define a new chaotic system using properties of both maps to generate 3D map with increased key space.

Chaotic maps are deterministic not probabilistic, this property also required in encryption systems, so that encryption and decryption can be done at both ends.

5.4.2 Limitations of Chaos-Based Cryptography

Although chaos – based cryptography has many advantages but there are certain limitations which do not suit practical implementation of these schemes.

Since these maps are iterative in nature hence very slow in computing the desired sequence. As seen in Table 5.1 with the increase in key length the time taken for calculation increases. Another reason for slow calculation is arithmetic operation over floating points, which increases number of clocks per operation as compared to integers.

As discussed in section 5.2 different types of processors generate different sequence for same input. Hence any cryptographic application of chaotic maps will produce wrong results at either end (Sender or Receiver).

Due to floating point arithmetic hardware implementation is also not suited because it requires huge resources and latency.

Discretization of values to a certain precision level decreases the behavior of dynamic systems. Chaotic maps are chaotic in nature and for calculations on computers they must be discretized to carry out with further calculations.

Another issue with chaotic maps is low key space. Although these maps exhibit aperiodic behavior but contain periodic orbits. To remain in chaotic region and one should not recognize the repeating pattern of attractor, well- experimented and analyzed values of control parameters are required to be selected. Hence control parameters define the region for chaos, and these control parameters alongwith variables define the key space. But with the reduction of periodic windows and correct selection of control parameters (with positive LE) key space reduces. When these schemes are tested under scenario with adversary then initial conditions of variable will also required to be excluded from key space if no transition algorithm mutually agreed upon between sender and receiver.

Increase in complexity of algorithm for bit generation increases the time taken for calculation. As conversion of real numbers to integers and then further conversion into bits stream require additional cycles to produce output.

5.5 Design Criterion for Chaos – Based Cryptography

After analyzing the cryptographic properties of chaotic maps and comparing some PRNGs some design criterion for chaos – based cryptography can be deduced.

Chaotic – Maps are not Cryptographic Primitive. Chaotic maps do not provide any cryptographic scheme building criteria. These can be used as PRNGs having good randomness properties. These PRNGs can further be utilized as nonce or key creation for different cryptographic primitives.

Real implementation should not degrade Chaotic properties. When chaotic maps are practically implemented then they lose their properties like aperiodic behavior against non - appropriate control parameters and initial conditions. Hence proper selection of discretization method tested against all worst scenario should be done before implementation.

Balance between Security and Speed. Chaotic functions are not only iterative but also involve arithmetic calculations of floating-point numbers. Hence while designing the chaotic schemes balances between currently available resources and security should be analyzed. Although increase in decimal points increases the key space but at same time become inefficient by consuming too much power and memory resources.

Key Space should be defined for a Specific Chaotic Implementation. Analysis part shows key space for effective chaotic region is reduced when optimization techniques are applied and does not produce that much of key length as defined for whole region for any proposed chaotic map. For current cryptography the security lies in public algorithm with computationally infeasible key space. With unknown key space it is never assumed that the cryptographic scheme is secure and there are always chances that adversary with higher resources can exploit the scheme. Hence while proposing any chaotic scheme effective key space should be defined against all parameters.

Correct Selection of values of Control Parameters and Initial Conditions. Before suggesting any chaos-based scheme all values of control parameters and initial conditions (précised values) should be checked for defining the effective key space. Maximum effective key space to be defined for the region which gives positive LE.

Attacks Resistant. Suggested schemes should test again all types of attacks from easier to difficult level. Even attacks with low complexity succeed although the scheme proved to be secure against very difficult and heavy attacks. Since chaotic maps do not define any primitive of cryptography and always implemented with some underlying primitive, hence all attacks against that primitives should also be analyzed in proposed schemes. Initial values of any scheme based on chaotic maps needed to be sent in clear in first transmission, so while doing analysis of attacks those parameters should not be included in defining the security like key space etc. However, the key size should always be resistant to brute-force attack.

Proposed Scheme to be Checked against All types of Processor. As discussed earlier, different processors produce different sequence with same initial conditions which hinders the implementation of chaos-based schemes. Hence proposed schemes should be tested on all types of processors so that both ends are at same level of satisfaction. It also necessary to define the specifications of machine against which the proposed scheme was tested for given outputs.

Chapter 6

Chaos – Based PKC in Post Quantum Era

6.1 Introduction

Post Quantum Era demands more secured primitives to be adopted in public key cryptography. After giving an overview of chaos-based PKC and developments in quantum computing, applicability of chaos-based cryptography will be analyzed in this chapter.

6.2 overview

Classical PKC is currently based upon Discrete Logarithm Problem (DLP) developed by Whitefield Diffie and Martin Hellman [15] as first key agreement protocol. However, they failed to provide mutual authentication between parties and later may protocols were developed to achieve authentication. Most known algorithm based upon DH is ElGamal [16]. Another algorithm based upon factorizing problem was introduced as RSA [17] and considered as difficult as DH to compute. After two years of DH in 1978 Merkle also proposed a PKC and known as Merkle's puzzle [18]. Contrary to currently in use PKC which is based on difficulties in the number theory and both keys (public and private) are predefined before starting communication, the Merkle's method depends on the protocol itself and both keys are defined by the transmitter at random.

Kocarev and Tasev [19] proposed a PKC scheme based on Chebyshev chaotic maps whose underlying crypto primitive was DH, but Bergamo et al. [20] proved insecurity of same as the Chebyshev equivalent trigonometric function is cosine and contains all points, hence adversary can recover plaintext from encrypted message without knowing the secret key.

Cocks [21] technique to encrypt message using variation of iterative function (IF) to get ID Based encryption proved to be inefficient due to bit by bit encryption, resulting into longer ciphertexts. Waters [22] and Boneh and Boyen [23] provided secure Identity based encryption without random oracle model. Lee and Liao [24] converted PKC using DL into IBC technique. Xiao et al. [25] key agreement protocol was countered by Han in

2008 [26] presented two attacks that enables an adversary to prevent the user and the server from establishing a shared key. Furthermore, in 2010, Wang and Zhao [27] proposed a modified chaos-based protocol which can be modified as illegal message as researched by Yoon and Jeon [28].

In 2009, Tseng et al. [29] gave the first key agreement protocol with user anonymity since earlier suggested protocols were not providing user anonymity. Niu and Wang [30] proved that it does not provide user anonymity, perfect forward secrecy, and security against an insider attacker, then proposed a new key agreement protocol. Soon, Yoon [31] proved that Niu-Wang's protocol is vulnerable to Denial of Service (DoS) attack and is fraught with computational problems.

Tseng and Jou [32] suggested a key agreement protocol based on chaotic maps, which allows users to interact with the server anonymously. From year 2012 Mesharm et al [33] proposed many ID based schemes, and in 2018 modified his work which used Chebyshev chaotic map- based ID – based cryptographic model using subtree and fuzzy-entity [34]. They proved that this model is secure under the IND-sST-CCA in the random oracle model and computational cost is very low.

In 2016 David Arroyo et al [35] did cryptanalysis of classical chaos – based cryptography having some quantum features proposed by Vidal et al, 2012 [36]. The proposed cryptosystem by Vidal et al was not efficient and key space reduces with optimization techniques and can be recovered by MITM. With reduction of key space, the brute force attack is possible with high speed computers. Hence once again the proposed scheme not secured against classical attacks.

These were two main underlying schemes for PKC based upon chaotic maps. If at all any scheme is secured against the classical attacks in current computation power the main problem with chaos based crypto system is low key space. This disadvantage exposes the schemes against quantum computers where brute force is enhanced by Grover’s algorithm and even symmetric encryptions with small keys are not secured.

All proposed schemes inherit the properties of either DH or factorizing problem and limitations of chaos - based cryptography as low speed and limited key space. According to Kirchhoff's principle security always invested in key and not in the hidden algorithm or protocol. currently threat of quantum computers and development of Shor's algorithm endangered most of the crypto schemes and specially the PKC. It is anticipated by most of the researchers that within eight years Shor's algorithm will be implemented at a relevant scale with the help of quantum computers. Hence, emerging technologies demand quantum resilient algorithms which can ensure privacy of sensitive data.

6.3 Quantum Computers and Cryptography

The two properties of quantum computing (superposition and entanglement) increased computation power and parallelism. To break any type of crypto scheme two types of attacks are used; i.e. reverse engineering and brute-force. Reverse engineering can only be done by exploiting the algorithm to find loop hole or trapdoor, while brute-force is extensive searching with all possibilities, a n – bit key crypto scheme can have n/2 operations to search a key on classical computer. So as far as symmetric encryption is considered it might not be affected by the quantum computers with longer keys. However, so far AES – 128 and AES – 256 are considered to have security of 64 bits and 128 bits as quantum security respectively. So, with the increase in key length the security level can be increased.

As far as PKC is concerned which is based upon factorizing problem, DLP and ECDSA are not considered secure with the development of Shor's and Grover's algorithms. It is assumed that with the increased computation power of quantum computers the PKC will vanish, since these are based on computation problems which are infeasible with current supercomputers. There is need to find other strong crypto primitives to build PKC instead of factorization and DLP based algorithms.

In 2016 NIST give call for post quantum PKC and In November 2017, 82 candidate submitted algorithms, 69 were considered and accepted with minimum acceptance criteria as First Round candidates. On January 30, 2019 NIST published a report for Second Round 26 candidates [37].

None of selected scheme is chaos – based, however, the primitives of these schemes are as under and none of these are also based upon factorization and DLP [38]:

1. Lattice-based Cryptography: It does matrices multiplication and based upon hardness of lattice problems and known as Short Vector Problem (SVP).
2. Multivariate-based Cryptography: The security of this public key scheme relies on the difficulty of solving systems of multivariate polynomials over finite fields. However, it is difficult to develop an encryption scheme based on multivariate equations. It can be used both for encryption and digital signatures.
3. Hash – Based Signatures: As it is considered as one-way function and assumed to be secured against quantum computation. However, random numbers generated for hash calculation can be chaotic maps based.
4. Code-based Cryptography: Code-based cryptography refers to cryptosystems that make use of error correcting codes. The algorithms are based on the difficulty of decoding linear codes and are considered robust to quantum attacks when the key sizes are increased by the factor of 4.

6.4 Conclusion

Quantum computers threats to cryptographic primitives is a concern in current era, since starting from highly secret official data of any country, business transaction, banking requirements and ending at the user's personal privacy and anonymity will be affected. Specially the high risk to PKC which is considered as core scheme for key sharing and agreement will no more be secured. Although chaotic maps provide good source of randomness and show aperiodic behavior which is desired property under classical cryptography, but its limitation of key space is big hurdle in its implementation. Key space of chaotic maps depends upon the number of parameters and the number of decimal places selected for key generation. With increase in number of parameters / axis and decimal places might increase key space but most of the chaotic maps used continuous maps which can also be defined by equivalent trigonometric function. Discrete time chaotic maps also face problem of key reduction when optimization techniques applied. NIST is working on post quantum cryptography since use of quantum channel for key transportation might not be practical for a layman using small devices with limited resources.

Chapter 7

Conclusion

Chaos theory was a new dimension introduced in field of cryptography two decades earlier with practical implementation in symmetric / asymmetric cryptography, random number generation, hash calculation and image / video encryption. Although Logistic equation was never considered secured for implementation in cryptography due to unimodal behavior, but later researchers worked on different types of chaotic maps starting from 1D maps to multidimensional maps. They exploited the basic properties of chaotic maps (ergodicity and sensitive to initial condition) to ensure security and increased number of control parameters and dimensions to increase key space. Unfortunately, the effective key space of these maps is short in length and these maps being iterative in nature have slow speed for generating the desired sequence.

For PRNGs these maps were used, and results were tested against different random number testing techniques. However, these random number testing techniques do not provide effective region or values for control parameters for which Lyapunov exponent and Bifurcation diagram are used. These methods effectively recognize the safe and effective region for any chaotic map under which control parameters can be varied. Low key space which is resulted due to presence of periodic windows, is a big disadvantage of chaotic maps, However, chaotic maps with enough key space like quantum chaotic map having key space of 236 bits is considered safe under current computation resources.

With the start of quantum computation era chaos-based cryptography used in symmetric encryption will be considered secure with key space equal or greater than 256, but chaos-based public key cryptography will also be under threat since underlying hard problem used in such schemes is DLP and ECDSA, which are insecure against quantum computation. However, with quantum computation issue of slow speed of these maps will reduce for computation of key and might also increase the key space as current computers do not allow discretization beyond defined value. Increase in key space can give an edge to beat the brute – force attack.

Whether classical computation or quantum computation successful encrypted data transfer means receiver has got the correct message and decrypted successfully. But in chaos-based cryptography arithmetic operation on floating point numbers have the limitation of generating different sequences on two different types of encrypting and decrypting engines. In quantum computers, leading quantum processor developers are IBM and Intel. Since IBM does not follow the IEEE-754 standard for arithmetic operations and decimal point numbers representation hence, two different processors like IBM and Intel would produce totally different number sequence same type of software implementation. This limitation restricts researchers and developers to use chaos-based cryptography as future cryptographic primitive. As future trend different post quantum cryptographic schemes specially, hashed based cryptography can use chaotic maps for key generation, provided key space is enough to beat Grover's algorithm with collision finding iterations $\sqrt[3]{}$ (N).

BIBLIOGRAPHY

[1] Science and Faith: An Evangelical Dialogue by Harry L. Poe and Jimmy H. Davis Nashville, Tennessee: Broadman and Holman Publishers, 2000. Copyright © 2000 by Harry L. Poe and Jimmy H. Davis.

[2] M.S. Baptista, "Cryptography with Chaos", 1998 Elsevier Science B.V.

[3] David Arroyo, Gonzalo Alvarez, Veronica Fernandez, "On the inadequacy of the logistic map for cryptographic applications", arXiv:0805.4355v1 [nlin.CD] 28 May 2008

[4] Anger Fog, "Chaotic Random Number Generators with Random Cycle Lengths", www.agner.org/random/theory, December 2000, revised November 25, 2001.

[5] Madhekar Suneel, " Cryptographic pseudo-random sequences from the chaotic Henon map", Sadhana Vol. 34, Part 5, October 2009, pp. 689–701. © Indian Academy of Sciences.

[6] Borislav Stoyanov, " Pseudo-random Bit Generation Algorithm Based on Chebyshev Polynomial and Tinkerbell Map", Applied Mathematical Sciences, Vol. 8, 2014, no. 125, 6205 – 6210, HIKARI Ltd.

[7] A. Akhshani, A. Akhavan, A. Mobaraki, S.C. Lim, Z. Hassan, " Pseudo random number generator based on quantum chaotic map," Article in Communications in Nonlinear Science and Numerical Simulation · January 2014.

[8] Ana Cristina DASCALESCU, Radu BORIGA, " A New Chaotic Dynamical System and Its Usage In A Novel Pseudorandom Number Generator With A Linear Feedback Register Structure", Proceedings Of The Romanian Academy, Series A, Volume 16, Special Issue 2015, pp. 357-366.

[9] Khalid Charif, Ahmed Drissi, Zine El Abidine Guennoun, " A Pseudo Random Number Generator Based on Chaotic Billiards", International Journal of Network Security, Vol.19, No.3, PP.479-486, May 2017 (DOI: 10.6633/IJNS.201703.19(3).17).

[10] Jeaneth Machicao, Odemir Martinez Bruno," Improving the pseudo-randomness properties of chaotic maps using deep-zoom", arXiv:1611.07539v2 [nlin.CD] 28 Dec 2016.

[11] Steven H. Strogaz," Book on Nonlinear Dynamics and Chaos".

[12] Intel Corporation, Intel°R 64 and IA-32 Architectures Optimization Reference Manual, 2009.

[13] https://en.wikipedia.org/wiki/IEEE_754

[14] A.N. Pisarchik and M. Zanin, Chaotic map Cryptography and Security.

[15] W. Diffie, M. Hellman, New directions in cryptography, IEEE transactions on Information Theory 22 (6) (1976)

[16] ElGmal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans Inform Theory*. 1995; 31:469-472.

[17] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM*. 1978; 21:120-126.

[18] R. C. Merkle, Commun. ACM **21**, 294 s1978d.

[19] L. Kocarev, Z. Tasev, Public-key encryption based on Chebyshev maps, in Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on, Vol. 3, IEEE, 2003.

[20] P. Bergamo, P. D'Arco, A. De Santis, L. Kocarev, Security of public-key cryptosystems based on Chebyshev polynomials, IEEE Transactions on Circuits and Systems I: Regular Papers 52 (7) (2005).

[21] Cocks C. *An identity-based encryption protocol based on quadratic residues*. *International Conference on Cryptography and Coding (Proceedings of IMA), Lecture Notes in Computer Science*. Vol 2260. Cirencester, UK: Springer-Verlag; 2001:360-363.

[22] Waters B. *Efficient identity-based encryption without random oracles*. *Advances in Cryptology-CRYPTO 2005*. Lecture Notes in Computer Science. Vol 3494.berlin: Springer-Verlag; 2005:114-127.

[23] Boneh D, Boyen X. *Efficient selective-id secure identity-based encryption without random oracles*. *Advances in Cryptology-EUROCRYPT 2004*. Lecture Notes in Computer Science. Vol 3027. Berlin: Springer-Verlag; 2004:223-238.

[24] Lee WC, Liao KC. Constructing identity-based cryptosystems for discrete logarithm-based cryptosystems. *J Netw Comput Appl*. 2004; 22:191-199.

[25] D. Xiao, X. Liao, S. Deng, A novel key agreement protocol based on chaotic maps, Information Sciences 177 (4) (2007) 1136-1142.

[26] S. Han, Security of a key agreement protocol based on chaotic maps, Chaos, Solitons & Fractals 38 (3) (2008).

[27] X. Wang, J. Zhao, "an improved key agreement protocol based on chaos", Communications in Nonlinear Science and Numerical Simulation 15 (12) (2010) 4052-4057.

[28] E.-J. Yoon, I.-S. Jeon, an efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map, Communications in Nonlinear Science and Numerical Simulation 16 (6) (2011) 2383-2389.

[29] H.-R. Tseng, R.-H. Jan, W. Yang, A chaotic maps-based key agreement protocol that preserves user anonymity, in: Communications, 2009. ICC'09. IEEE International Conference on, IEEE, 2009, pp. 1-6.

[30] Y. Niu, X. Wang, an anonymous key agreement protocol based on chaotic maps, Communications in Nonlinear Science and Numerical Simulation 16 (4) (2011) 1986-1992.

[31] E.-J. Yoon, Efficiency and security problems of anonymous key agreement protocol based on chaotic maps, Communications in Nonlinear Science and Numerical Simulation 17 (7) (2012) 2735-2740.

[32] H.-R. Tseng, E. Jou, an efficient anonymous key agreement protocol based on chaotic maps, in: High Performance Computing and Communications (HPCC), 2011 IEEE 13th International Conference on, IEEE, 2011, pp.752-757.

[33] Meshram C, Meshram S, Zhang M. An ID-based cryptographic mechanism based on GDLP and IFP. *Inf Process Lett*. 2012;112(19):753-758.

[34] Mesharm C, Mesharm S and Obaidat M.S. Chebyshev chaotic map-based ID-based cryptographic model using subtree and fuzzy-entity data sharing for public key cryptography. Jan 2018. DOI: 10.1002/spy2.12

[35] D. Arroyo, F. Hernandez, A.B. Orue. Cryptanalysis of classical chaos – based cryptography with some quantum features. arXiv:1610.08475v1 [cs.CR] 26 Oct 2016

[36] Vidal, G., Baptista, M. S. & Mancini, H. [2012] "Fundamentals of a classical chaos-based cryptosystem with some quantum cryptography features," International Journal of Bifurcation and Chaos 22, Article number 1250243.

[37] https://doi.org/10.6028/NIST.IR.8240

[38] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang. The Impact of Quantum Computing on Present Cryptography. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3, 2018. arXiv:1804.00200v1[cs.CR] 31 Mar 2018.

[39] M. Hamdi, R. Rhouma and S. Belghtith. "A Very Efficient Pseudo-Random Number Generator Based on Chaotic Maps and S-Box Tables". World Academy of Science, Engineering and Technology, International Journal of Electronics and Communication Engineering, Vol:9, No:2, 2015.

[40] L. Merah, A-P. Adda and H. Naima, "Enhanced Chaos – Based Pseudo Random Numbers Generator". 2018 International Conference on Applied Smart Systems (ICASS'2018). 24-25 November 2018, Medea, ALGERIA

[41] Li, Shujun, Guanrong Chen, and Xuanqin Mou." On the dynamical degradation of digital piecewise linear chaotic maps." International Journal of Bifurcation and Chaos 15.10 (2005): 3119-3151.