ISSN:0975-9646

Analysis of Crypto Components of a Chaotic Function to Study its Random Behavior

Kangkana Bora[#1], Abdul Wadood[*2], Mayur Hazarika[#3], Zahid Ahmed[*4]

[#1]*Assistant Professor, Department of Computer Science,*
Regional Institute of Science and Technology, Meghalaya

[*2, #3,*4] *B.Tech student, Department of Computer Science,*
Regional Institute of Science and Technology, Meghalaya

Abstract - **Chaos theory is the study of dynamic systems that evolve in time presenting properties such ergodicity, sensitivity to initial conditions, topological mixing etc. A remarkable characteristic of chaotic systems is their capability of producing quite complex patterns of behavior from simple real systems which makes it suitable to be used in cryptosystems.**

This paper presents an overview of an analysis of the parameters affecting the chaos function which may indirectly affect the cryptographic system under consideration. It has been a great challenge over the last few years to determine the appropriate parameter values that give the highest randomness.

Keywords - **Chaos theory, cryptography.**

I. INTRODUCTION

Ever since the discovery of chaotic behavior in the mathematical models of weather systems by Edward Lorenz in the early 1960s [1], chaos theory has been a common theory in various fields including physics, biology, economics and even philosophy. In the last couple of decades, chaos theory has been greatly influencing the field of cryptography as the main principle of a perfect cryptosystem is to generate the most complex key to encrypt the plaintext.

This paper looks around the nature of chaos based cryptosystem and analyses the ranges and limitations of values which can be provided to the chaotic logistic equation.

II. CHAOS BASED CRYPTOSYSTEM

Consider the following logistic equation of a chaos system

$X_{n+1}= r X_n(1-X_n)$; r Ɛ(3,4) and X_n Ɛ(0,1) (1)

Chaos systems have certain characteristics that can be related to some of the important properties a cryptosystem which make chaos systems applicable to cryptography.

1. Ergodicity :

Statistical measurements of the variables give similar results no matter if they are performed over time or space [2]. The output of the system seems similar for any input even if they are different. This characteristic is similar to the “confusion” property of cryptosystem which ensures that the cipher text does not reveal the plaintext.

2. Sensitivity to initial condition :

Given an initial state of a deterministic system, it is well known that the future states of the system can be predicted. However, for chaotic systems, long term prediction is impossible. For specific values of parameters, two trajectories, which are initially very close, diverge exponentially in a short time. Initial information about the system is thus completely lost [3],which is the concept of “diffusion” in cryptography that is used to mean an increased redundancy of plaintext by spreading it across rows and columns.

3. Topological mixing :

It means that the system will evolve in time so that any given region of states is always transformed or overlaps with any other given region [2]. Self-mapping of functional values over iterations makes it distributed over the whole space. This characteristic is similar to the “multi-round transformation” concept of cryptography which transforms the bit positions of the plaintext.

A. Analysis of crypto components :

The most challenging part of the chaos system is to determine the appropriate values and ranges of the parameters included in the logistic function that is the initial value and r value. In most of the previously published papers[1][2][3][4][5][6][7], the range of values for r is (3,4), and that of initial parameter X_n is (0,1), but they did not mention satisfactorily the reasons why they are varied to these limits only.

1. Analysis of r :

The parameter ‘r’ is a factor that greatly affects the logistic equation. As per our findings the values of ‘r’ varies from 1 to 4.2. The reason for not taking more than 4.2 is that if we give those values of ‘r’ in the logistic equation, it gives undefined values to the function for most of the iterations. For example, the values x after each iterations for r =4.3 are as follows:

```
0.3869999999999999
1.0200932999999999
-0.0881372750310264
-0.4123934534079611
-2.5045857994333325
-37.743404052472684
 -6287.924200138941
-1.7004039828484026E8
-1.24329070041302256E17
-6.646818592654068E34
-1.8997484883570277E70
-1.551889057176369E141
-1.0355946476870168E283
```

-Infinity
-Infinity
-Infinity
-Infinity
-Infinity
-Infinity

The figures below shows the nature of randomness for different values of r

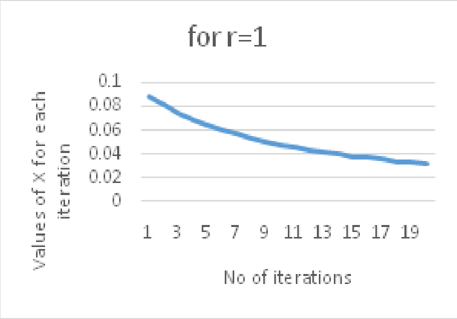

Fig 1. Graph with r value 1

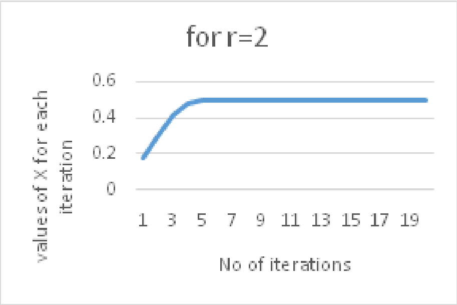

Fig 2. Graph with r value 2

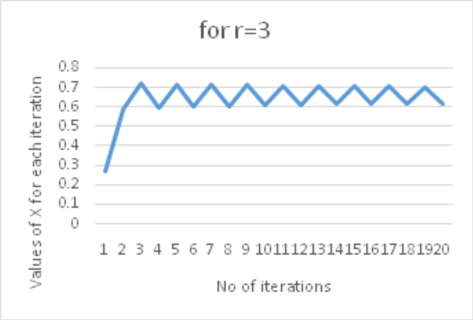

Fig 3. Graph with r value 3

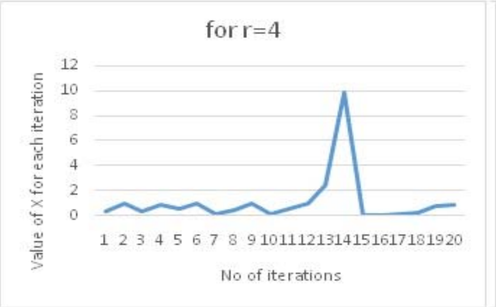

Fig 4. Graph with r value 4

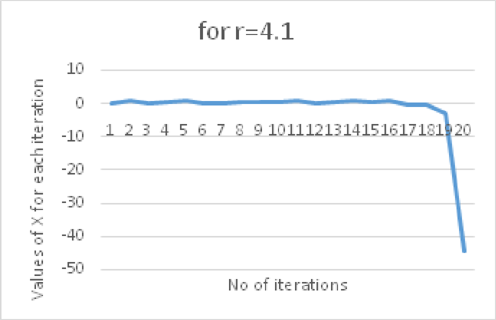

Fig 5. Graph with r value 4.1

Form the above graphs for different values of 'r', the logistic equation shows more randomness when r Ɛ(3,4) and for r =4 and beyond 4 the randomness becomes less. That is the reason why most researchers concentrate on the range 3-4.

To study the randomness we considered the concept of standard deviation using the formula-

$$S = \surd\ (X\text{-}X')^2/(n-1) \qquad (2)$$

Where X = each score
X' = the mean or average
n = the number of values
∑ means the sum across the values

It is said that more the Standard deviation more will be randomness. The standard deviation for distribution of x values keeping r value fixed are as shown in the Table I.

TABLE I
STANDARD DEVIATION FOR DISTRIBUTION OF X VALUES KEEPING R VALUE FIXED (INITIAL VALUE TAKEN IS 0.9)

r values	Standard deviation
1	0.0166541
2	0.0812905
3	0.0991434
3.1	0.1164614
3.2	0.1357884
3.3	0.1382067
3.4	0.1739956
3.5	0.2053754
3.6	0.2222499
3.7	0.2136420
3.8	0.2599768
3.9	0.2726017
4	2.0877335

From the above observation it can be said that standard deviation is increasing from r=1 to 4. So r value giving highest standard deviation value is preferred.

2. *Analysis of Initial value:*

Initial value parameter is another factor that determines the chaotic nature of the logistic equation. The values of initial value X_n varies between 0 and 1. The reason for not allowing more than 1 in its values is that if we take more than 1 the logistic equation results in unpredictable values for the iterations. For example if we take X_n = 2 then corresponding X value after each iterations are-

X_1= 7.862920240164593E23
X_2= -2.4730205881276004E48
X_3 -2.446332331721193E97
X_4 -2.39381675088978E195
X_5 -Infinity
X_6 -Infinity
X_7 -Infinity
X_8 –Infinity and so on...

The standard deviation for distribution of x values keeping initial value fixed and r value as 3 are as shown in the Table II.

TABLE II
STANDARD DEVIATION FOR DISTRIBUTION OF X VALUES KEEPING INITIAL VALUE FIXED (R VALUE TAKEN IS 3)

Values of Initial X_n	Standard deviation
0.1	0.099180
0.2	0.0743054
0.3	0.0318138
0.4	0.0472701
0.5	0.0636953
0.6	0.0472700
0.7	0.0318138
0.8	0.0741372
0.9	0.0991434

From the above observation it can be said that standard deviation is increasing from initial value=0.1 to 0.9. So initial value giving highest standard deviation value is preferred.

III. CONCLUSSION

Digital chaotic ciphers have been investigated for more than a decade. However, their overall performance in terms of the tradeoff between security and speed, as well as the connection between chaos and cryptography, has not been sufficiently addressed [4]. The main focus of this approach is to examine the parameters from cryptographic point of view so that it can help in designing secured cryptographic encryption system.

Some idea for further enhancement include- designing a symmetric and asymmetric key encryption algorithm using suitable parameters and comparisons with already exited systems.

REFERENCES:

[1] Christopher A. Wood, *Chaos-Based Symmetric Key Cryptosystems*, Department of Computer Science, Rochester Institute of Technology, Rochester, New York, USA. Available: http://www.worldcomp-proceedings.com/proc/p2011/SAM8575.pdf.

[2] Pellicer-Lostao Carmen, López-Ruiz Ricardo Notions of *Chaotic Cryptography: Sketch of a Chaos based Cryptosystem,* Department of Computer Science and BIFI, University of Zaragoza, Spain.Available on http://arxiv.org/ftp/arxiv/papers/1203/1203.4134.pdf.

[3] Q.V. Lawande, B. R. Ivan,S. D. Dhodapkar,*Chaos Based Cryptography : A New Approach To Secure Communications, BARC newsletter, No 258, June 2005,*Theoretical Physics Division.

[4] Masuda N., Jakimoski, *Chaotic Block Cipher:from Theory to Practical Approach,* Circuits and System I, IEEE transaction, volume 53, issue 6, page 1341-1352,ISSN 1549-8328.

[5] Kamel Faraoun, *Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption,* Département d'informatique, UDL University, Algeria, The International Arab Journal of Information Technology, Vol. 7, No. 3, July 2010, pg-231-240.

[6] Bassem Bakhache, Kassem Ahmad, Safwan el Assad, *A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi networks* , International Journal of Intelligence Computing research, Informatics Society, Volume 2 issue 4, Dec 2011, pg 220-227.