Pseudo – Random Number Generator Using Deterministic Chaotic System

Mohamed Nageb Elsherbeny, Mahmud Rahal

Abstract:- A new Iteration Function System (IFS) is used to generate a Pseudo - Random Number Generator. The sensitivity of the Iterated Function System (IFS) to the initial condition is measured. At certain initial value, the iterated function (IFS) can generate a chaotic random numbers. This generator is very useful and can be used as a key in a crypto- system algorithms.

Index Terms:- Key, Crypto-Systems, Chaotic, Randomness, Statistical Tests, Generator, Cryptography.

1. INTRODUCTION

Random number generators (RNG) are useful in every scientific area. Extremely important is the application of RNGs in cryptography for the generation of cryptographic keys [1]. The choice of the RNG for a specific application depends on the requirements specific to the given application. If the ability to regenerate the random sequence is of crucial significance or the randomness requirements are very stringent then one should resort to pseudo – random number generator (PRNGs). PRNGs algorithms are capable of generating sequences of numbers which appear random – like from many aspects. Though they are necessarily periodic and their periods are very long, they pass many statistical tests and can be easily implemented with simple software routines [12]. The cipher requires a truly random sequence and PRNGs are appropriate for such a purpose. It is necessary that cryptographic keys and initialization variables in cryptographic protocols are generated by RNGs. It is widely accepted that the core of any RNG must be an intrinsically random physical process such as tossing a coin, throwing a dice [2], drawing from a urn, drawing from a deck of cards and spinning a roulette, measuring thermal noise from a resistor and shot noise from zener diode [3] – [6], measuring active decay from radioactive source [7]. There exist certain methods to convert the assumed randomness of a physical process into a sequence of discrete random variables. These methods introduce biases in the binary sequence. The assumed randomness of the physical process is checked using statistical tests [7]. Practically, no finite number of statistical tests can prove that a sequence is random. Theory and tools of nonlinear systems and chaotic behavior have provided alternative and qualitatively different types of RNGs. Several authors have already proposed to use chaotic systems sources of physical randomness [8] – [9]. Chaos theory plays an active role in the improvement of the quality of PRNGs [5]. The advantage of using chaos in this field lies in its disordered behavior and its unpredictability.

- Mohamed Nageb Elsherbeny, Assistant Prof., King Saud University, Teacher college, Computer Department , Saudia Arabia.
  E-mail: mnageb@ksu.edu.sa
- Mahmud Rahal ,Associate Prof., King Saud University , Teacher college , Computer Department, Saudia Arabia.
  E-mail: mrahal@ksu.edu.sa

Chaotic system is defined on real / complex numbers spaces (bounded continuous space) whereas cryptography focuses on the properties of the iteration [10]. The modern of chaos is connected with the behavior of dynamical systems that appear to exhibit erratic and non – predictable behavior. A key feature of chaotic behavior in different systems is the sensitivity to initial conditions. Thus, it may happen that small differences in the initial conditions produce very great ones in the final phenomena. This aspect of a chaotic system is ideal for encryption since the cryptographic system should highly be based on to the initial conditions (key) that applied [11]. Chaotic systems are commonly based on recursive processes, either in the form of single or coupled algebraic equations.

2. PROPERTIES OF CHAOTIC SYSTEMS REQUIRED FOR CRYPTOGRAPHY.

1) It is impossible to predict the behavior of the **chaotic** system even if we have partial knowledge of its organization [10].
2) The state point stays within a bounded state space approaches infinitely closely to any point of the state space.
3) To create deterministic chaotic system :
   3.1. Define an IFS f(x)
   3.2. Input initial condition x_0 and parameter r
   3.3. Output is a sequence of states $x_1, x_2, x_3, \ldots$where $x_{i+1} = f(x_i, r)$
   3.4. Stability of an iteration process:

To measure the sensitivity of an iterated function to the initial function (key) [Lyapunov Exponent λ]:

$$\lambda(x_0) = \lim_{N\to\infty}\left(\frac{1}{N}\sum_{n=1}^{N} \ln |f'(x_n)|\right)$$

The required exponent (λ) is:

- $\lambda > 0$ (chaotic behavior)
- λ approaches 1 (extent of chaoticity)

3. NEW DETERMINISTIC CHAOTIC SYSTEM

$\mathbf{q = p * x_{i-1}}$

$s = cos(q) - \sin(q)$

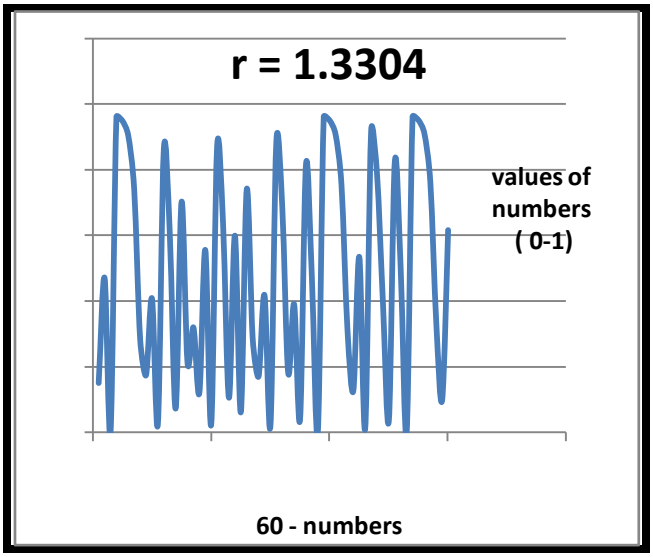
$s1 = tan(q + p/2)$

$\mathbf{x_I = r * |s| / (h + |s_1|)}$

$\mathbf{p = 1.605 , h = 0.344}$

The following table shows the numbers generated at the following initial conditions:

The following graph shows the behavior and the distribution of the generated random numbers using the above iterated function system.



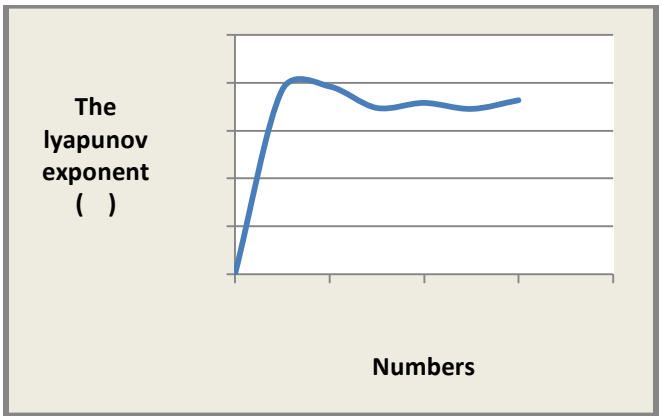
The usual test for chaos is calculation of the largest Lyapunov exponent: The following table shows the values of Lyapunov exponent (λ) of the above iterated function to the initial condition $x_o = 0.3$:

0	0
10	0.77168
20	0.786222
30	0.696331
40	0.717331
50	0.692229
60	0.728485

$x_0 = 0.3 , r = 1.3304$

0.150754	0.471091	0.000669	0.962304	0.950382
0.904641	0.740269	0.285348	0.174753	0.40837
0.0266	0.864783	0.610853	0.073106	0.703462
0.21169	0.320173	0.120449	0.556396	0.024288
0.873253	0.637308	0.10572	0.600332	0.06173
0.741354	0.287675	0.170831	0.418329	0.020123
0.888623	0.686748	0.181682	0.391057	0.039906
0.816879	0.471663	0.0006	0.962573	0.951429
0.908608	0.753842	0.315117	0.127744	0.535236
0.012218	0.918184	0.787136	0.394051	0.037421
0.825716	0.49602	0.000555	0.962744	0.952096
0.911138	0.762569	0.334994	0.100233	0.61712

The following graph measures the lyapunov exponent (stability of the above iterated function λ) :



From the above figure we see that the largest lyapunov exponent $\lambda = 0.728485$

From this result we deduce that the above iterated function (IFS) has a chaotic behavior.

4.
5.
6.

CONCLUTION

We suggest an iterative function system (IFS) which produces random numbers. These numbers have a chaotic behavior so it is impossible to predict the behavior of the system even if we have partial knowledge of its organization. This generator can be used usefully as a key generator in different crypto – system algorithms.

King Saud University, Teachers College, computer Department

ACKNOWLEDGMENT.

The authors extend their appreciation to the Research center of Teacher college, King Saud University for funding this work through the research group project No RGP-TCR-30 .

REFRENCES

[1] H.Niederreiter , Random Number Generator and Quasi – Monte Carlo Methods .Philae Phial , PA:SIAM, 1992

[2] S.M.Mathyas and C.H.Meyer "Generation, Distribution and Installation of Cryptographic Keys" IBM Syst.J, Vol 17, No2,1978

[3] C.H.Vincent," The generation of truly random binary numbers," J, Physics E, vol 3 , 1970.

[4] R.S.Maddocks, S.Matthews,E.W.Walkes,and C.H.Vicent,"A compact and accurate generator for truly random number binary digit" J.Physics E,vol.5,1972

[5] H.F.Murry," A general approach for generating natural random variables " IEEE Trans.Comput,vol.19,1970

[6] W. T. Holman, J. A. Cannelly, and A. B. Dowlatebad, "An integrated analog / digital noise source ," IEEE Trans. circuits syst. vol. 44,1997

[7] Toni Stojanovski and Ljupco Kocarev, Senior Member , " Fundamental theory and applications," IEEE Trans. On circuits and syst., Vol. 48, 2001.

[8] G. M. Bernstein and M. A. Lieberman, "Secure random number generation using chaotic circuits," IEEE Trans. Circuits syst.,vol.37,1990

[9] M. delgado-Restituto, A. Rodriguez, S. Espejo, and I. L. Huertas," A chaotic switched – capacitor circuits for 1/f noise generation," IEEE Trans.Circuits Syst., vol.9,1992.

[10] J M blackledge, "Cryptography using chaos," Cryptography using chaos", Warsaw University of Technology Development Programme, 2010.

[11] Cambel, A , B , "Applied Chaos Theory", Goman, 2000

[12] Institute for theoretical physics ETH Zurich, Diploma Thesis, "A Random Number Generator Test Suite for the C++ Standard", Mario Rutti, March 10, 2004.