A NEW METHOD TO IMPROVE THE SAFETY AND THE RANDOMNESS OF A PSEUDORANDOM BIT GENERATOR BASED ON A CHAOTIC MAP

Lect. Ana Cristina Dăscălescu, PhD student
Titu Maiorescu University, Faculty of Computer Science, Bucharest
cristina.dascalescu@utm.ro

Abstract

Chaotic cryptology is widely investigated recently. This paper reviews the progress in this area and points out some existent problems in digital chaotic ciphers like the predictability of the generated values using the orbits of a sole system and the low space of the keys. As a comprehensive solution to these problems, a novel method based on a composition of chaotic systems is presented. We will prove, using mathematically concepts from discrete dynamical nonlinear systems, that the composition of chaotic maps preserves and, moreover, improves the chaotic behavior of a single map. Also we present a detailed theoretical and statistical analysis for a pseudo number generator based on the proposed method. It is show that it has perfect cryptographic properties, and it can be used to construct stream ciphers with higher security. Some experiments are made for confirmation.

Keywords: chaotic systems**,** pseudo random, chaotic maps, stream cipher.

1. Introduction and motivation

In the last decade, the relationship between chaos and the classic cryptography has been highlighted and intensely analyzed because several properties of the non-linear dynamic systems have a correspondent among encryption systems based on computational methods. Thus, characteristics of the chaotic systems such as ergodicity, system's sensitivity to the initial condition or the parameters' values, the mixing property, the deterministic dynamic and system's complexity, are similar to the properties given by the diffusion to minor changes of the plain or in key text, the diffusion determined by a change of the plain text, the deterministic pseudo-randomness and the complexity of the algorithm from the classic encryption systems [9].

From the year 2000 onwards, based on these results, a series of chaos-based cryptosystems have been proposed, such as: block type symmetric systems based on the construction of encryption keys from the system's initial conditions, the string type symmetric systems based on the generation of random sequences to mask the plaintext, etc [3,4,5].

However, the vulnerability of these systems shouldn't be neglected. Some of the proposed chaos-based cryptosystems haven't resist to certain types of cryptanalytic attack. The predictability of the generated values using the orbits of a sole system and the low space of the keys, allow attackers' to easily extract the information about the system, making the chaos-based encryption systems to be weak candidates for security applications of the information. For a chaotic cryptosystem to resist to this type of attack, it has been recently proposed to combine multiple chaotic systems.[7,8] . Another important issue to be considered in creating a chaotic cryptosystems is generated by the relatively low space of the encryption keys.

The behavior in time of the chaotic systems strictly depends on the choice of parameters and the initial value (seed). Thus, for *the logistic map* $f_L: [0,1] \to [0,1], f_L(x) = rx(1-x), \forall x \in [0,1]$, the chaotic behavior is ensured for a set of the parameter's values in the range (3.9, 4]. Another category of functions, preferred for the simplicity and performances offered in cryptographic applications, is represented by *tent map*: $f_T(x): [0,1] \to [0,1]$,

$$f_T = \begin{cases} 2kx, & 0 \le x \le \frac{1}{2} \\ 2k(1-x), & \frac{1}{2} < x \le 1 \end{cases} \quad (1)$$

The chaotic behavior of the tent map is also ensured for a small set of parameter's values, in the range [0.7, 1].

This article proposes a new solution to eliminate the negative aspects presented above. To this end, it is analyzed and presented a new pseudorandom number generator which is based on composition of several logistic type functions, which has good cryptographic qualities and can be successfully used to create keystreams for a symmetric cryptographic system.

2. The logistic map

The most studied and used chaotic map within the specialty on dynamic and chaos systems is the *logistic map*, described by the recurrence:

$x(n+1) = f_L(x(n))$,

where f_L: [0,1] → [0,1] is defined through:

$$f_L(x) = rx(1-x), \forall x \in [0,1] \quad (2)$$

The behavior in time of the logistic map depends on the value of the parameter *r* and the starting point represented by the initial condition $x_0 = 0.7$. In figure 1 we have summarized the complete dynamical behavior of the logistic map using the *bifurcation diagram*.

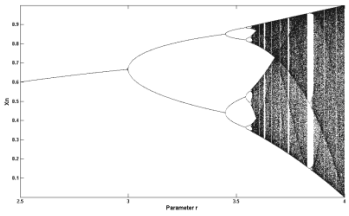

Figure 1. Bifurcation diagram of the logistic map

Analyzing the diagram, it can be noticed that for a data set of the parameter in the interval (3.9, 4] the logistic map has a chaotic behavior. Anyway, it can be noticed that within this interval, the function has areas with periodic behavior.

It is has been shown analytically that for the logistic map with system parameter $r = 4$, the distribution probability is given by $\varphi_f = \frac{1}{\pi\sqrt{x(1-x)}}$. [1] (3)

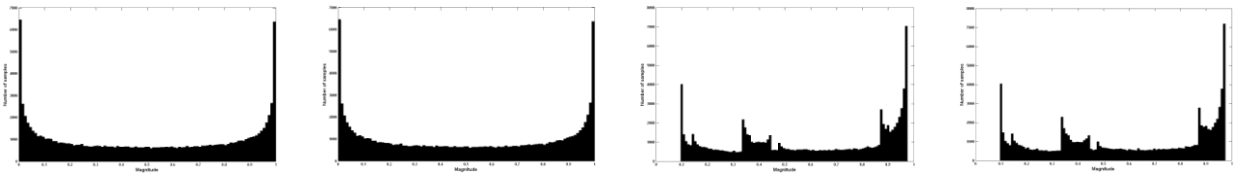

Figure 2. Histograms of the logistic map with:
(a) $r = 4$ and $x_0 = 0.1$ (b) $r = 4$ and $x_0' = 0.9$ (c) $r = 3.9$ and $x_0 = 0.1$ (d) $r = 3.9$ and $x_0' = 0.9$

Figures 2(a) and 2(b) present the distribution probability of the logistic map trajectories, which start from different initial conditions $x_0 = 0.1$ and $x_0' = 0.9$, with the system's parameter $r = 4$. Here, the interval [0, 1] has been spilt in 100 subintervals, and for each trajectory a total of N=10^5 point has been used. It can be noticed that the two distributions are identical and the logistic map keeps an invariant density if $r = 4$. Besides, the distribution probability is symmetric to the halfway point of the interval [0, 1]. Figures 2(c) and 2(d) show the distribution probabilities for two trajectories which starts from different points $x_0 = 0.1$ and $x_0' = 0.9$ with system's parameter $r = 3.9$. We can say that the logistic map still keeps an invariant distribution density, but is no longer symmetric to the 0.5.

Analyzing the two figures 2(a) and 2(b) we can conclude that the logistic map is surjective on the interval [0, 1], only for values of the parameter *r* that are very close to r = 4. The existence of the invariant distribution allows the substitution of time average with space average (ergodicity). This property allows an analytic computing of the Lyapunov exponent for the logistic map with the parameter $r = 4$, through relation:

$$L = \int_0^1 P(x)\lambda(X)dX, \tag{4}$$

where $\lambda(x)$ is the local Lyapunov exponent. From (5) and (6) results [5]:

$$L = \int_0^1 \frac{1}{\pi\sqrt{x(1-x)}} \ln\left|f'(x)\right| dx, = \int_0^1 \frac{1}{\pi\sqrt{x(1-x)}} \ln|4(1-2x)|\, dx = ln2$$

The positive value of the Lyapunov exponent confirms the chaotic nature of the logistic map for $r = 4$. In figure 3 is represented the Lyapunov exponent for parameter's values $r \in [1,4]$.

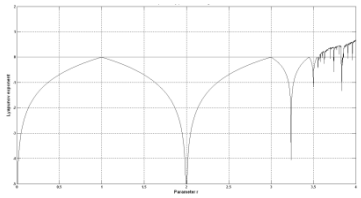

Figure 3. Lyapunov exponent of the logistic map

In the next chapter is presented the basic terminology for the proposed method. We will prove, using mathematically concepts from discrete dynamical nonlinear systems, that the composition of chaotic maps preserves and, moreover, improves the chaotic behavior of a single map.

3. The proposed method

In section 1 we have discussed that such chaotic pseudorandom number generators (PRNGs) are potentially insecure, since their output may expose some information about chaotic systems. In this paper, we present a new PRNG based on a composition of chaotic logistic diagrams with different parameters, which can provide higher security than other ciphers due to the fact that more chaotic systems are used to generate PRN.

Let's suppose that we have *k* type logistic maps with different parameters: $f_1(x_1, r_1), f_2(x_2, r_2), \dots, f_k(x_k, r_k)$, where $r_1, r_2, \dots, r_k$are control parameters and $x_1(0), x_2(0), \dots, x_n(0)$ are the initial conditions which determine *k* chaotic orbits. Hereinafter, we will study the chaotic properties of the function:

$$F_k(x) = f_1 \circ f_2 \circ \dots \circ f_k. \tag{5}$$

For $k = 2$, the function

$$F_2(x) = f_1(x, r1) \circ f_2(x, r_2) = r_1 * r_2 * x * (1-x) * [1 - r_2 * x * (1-x)] \tag{6}$$

is obtained.

In order to find the invariant density measure for the fof map, we briefly describe next a construction method for the invariant measures of the logistic map $f(x) = 4x(1-x)$. It was shown that the logistic map and tent map (1) are topologically conjugated by the function [1]:

$$C(x) = (1 - cos\pi x)/2 \tag{7}$$

which means that the relation :

$$f^{\circ}C = C^{\circ}T \tag{8}$$

is satisfied.

It was proved that the tent map keeps an invariant density, which is $\varphi_T(x) = 1$. In other words, for

$$\mu(x) = \int_0^x \varphi(x)dx = \mu(S) = \int_{C^{-1}(s)} 1\, dx.\,, \quad \forall x \in [0,1] \tag{9}$$

we have $\mu(X) = \mu(F^{-1}(X))$, for any set $X \subset [0,1]$.
Applying the change of the variable $y = (1 - cox\pi x)/2$, we rewrite the relation (9) through the integral $\int_S \frac{1}{\pi\sqrt{y(1-y)}}dy$, witch leads us at the invariant density for the logistic map $\varphi_f = \frac{1}{\pi\sqrt{x(1-x)}}$. [1].

In order to demonstrate that the function $f^{\circ}f$ preserves too an absolutely continuous invariant density, we apply the same method. Thus, to verify that fof and ToT are topologically conjugated by the $C(x)$ map, we need to check if $f^{\circ}f^{\circ}C = C^{\circ}(T^{\circ}T)$. A result is shown only for $0 \le x \le 1/2$. The left side is

$$f((f\big(C(x)\big) = f(sin^2\pi x) = 4sin^2\pi x(1 - sin^2\pi x) = sin^2 2\pi x \tag{10}$$

For the right side, we use the fact that T(x) = 2x for $0 \le x \le 1/2$, so that

$$C(T(T(x))) = \frac{1-cos\pi T(x)}{2} = \frac{1-cos4\pi x}{2} = sin^2 2\pi x \tag{11}$$

We conclude that the map preserved an absolutely continuous invariant density, which is $\varphi_f = \frac{1}{\pi\sqrt{x(1-x)}}$.

For the relation (8), we'll apply the composing operation of k order, from where it results the following identity:

$$f^k(x)^{\circ}C(x) = C(x)^{\circ}T^k(x) \tag{12}$$

Thus, we can say that the function $f^k(x)$, keeps the same invariant density $\varphi_f = \frac{1}{\pi\sqrt{x(1-x)}}$, for parameters $r_1 = r_2 = \cdots = r_k = 4$.

Hereinafter, we analyze the distribution of the trajectories generated by the function F_2, defined in (6), for which $r_1 = 4$ and $r_2 \in [1,4]$, so we can redefine the function F_2through relation :

$$F_2(x) = f_1(x,4)^{\circ}f_2(x,r_2) = 4 * r_2 * x * (1-x) * [1 - r_2 * x * (1-x)] \tag{13}$$

In the following we will consider the function $F_2(x)$ defined in (13) as a one-dimensional function with a single parameter r_2.

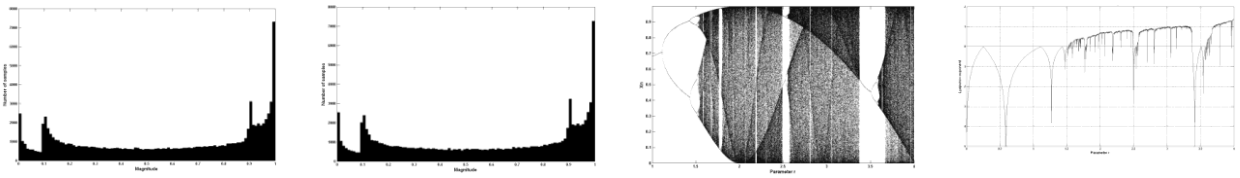

Figure 4. Analysis of the function F_2:

(a) Histogram for $r_2 = 3.9$ and $x_0 = 0.1$ (b) Histogram for $r = 3.9$ and $x_0' = 0.9$ (c) The bifurcation diagram (d) The Lyapunov exponent

In figures 4(a) and 4(b) are represented the distributions probabilities of the type F_2 functions trajectories, which start from different initial conditions $x_0 = 0.1$ and $x_0' = 0.9$, with the system's parameter $r_2 = 3.9$. Here, the interval [0, 1] has been split in 100 subintervals and for each trajectory a total of N=10^5 points have been used. It is obvious that the two distributions are identical, so the F_2 function with parameters $r_1 = 4$ and $r_2 = 3.9$ and preserve an invariant density. Also, must be highlighted that the F_2 function is surjective in the interval [0, 1] for the parameter $r_2 = 3.9$.

The behavior in time of the function F_2 depends on the value of the parameter r_2 and on the starting point represented by the initial condition $x_0 = 0.7$. In figure 4(c), we have summarized the complete dynamical behavior of the F_2 using the bifurcation diagram. Analyzing the diagram, it can be observed that for the parameter's data set in a range of [3.6, 4] the F_2 function has a chaotic behavior.

In figure 4(d) we have displayed the Lyapunov exponent. The results are most interesting since it is obvious that the is positive for a larger interval of values than in the case of parameter r_2. We can conclude that the F_2 map have a better chaotic behavior for several values of the system's parameter, which means that the very narrow key space of the logistic map was improved. Moreover, the cryptanalyst cannot easily extract the information about the system's chaotic behavior because the output is obtained from two chaotic orbits.

We go forward with our analysis and try to obtain some results for values $k = 4$ and $k = 8$, for relation (5). Thus, we present the analysis for functions F_4 and F_8 defined as:

$$F_4 = f_1(x,4)\circ f_2(x,4)\circ f_3(x,4)\circ f_4(x,r_4) \quad (12)$$

$$F_8 = f_1(x,4)\circ f_2(x,4)\circ f_3(x,4)\circ f_4(x,r_4)\circ f_5(x,4)\circ f_6(x,4)\circ f_7(x,4)\circ f_8(x,r_8) \quad (13)$$

The above defined functions, F_4 si F_8 are interpreted as one-dimensional functions with a single parameter r_4, respectively r_8, which varies in the range [1, 4].

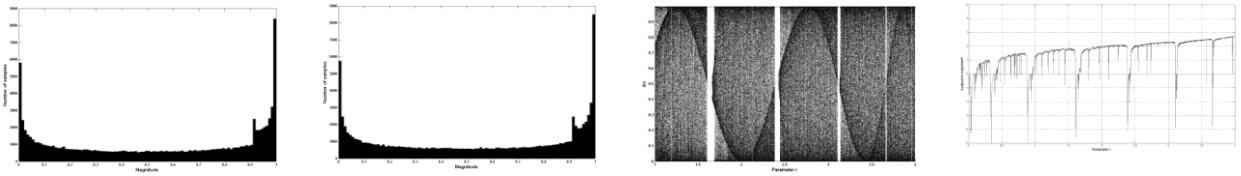

Figure 4. Analysis of the function F_4:

(c) Histogram for $r_2 = 3.9$ and $x_0 = 0.1$ (d) Histogram for $r = 3.9$ and $x_0' = 0.9$ (c) The bifurcation diagram (d) The Lyapunov exponent

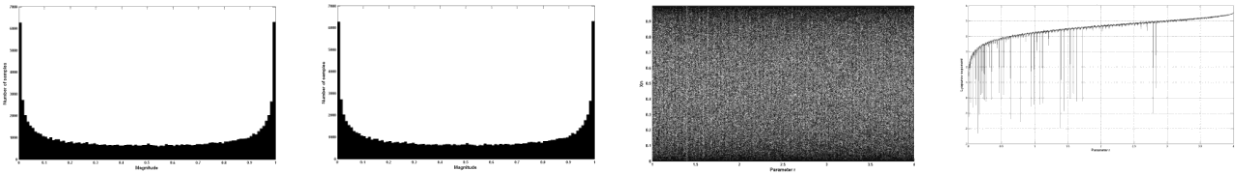

Figure 4. Analysis of the function F_8:

(e) Histogram for (f) Histogram for (c) The bifurcation (d) The Lyapunov

$r_2 = 3.9$ and $x_0 = 0.1$ $r = 3.9$ and $x_0' = 0.9$ diagram exponent

In a similar way as above, in the figures 5(a-d) and 6(a-d) are represented the trajectories' distributions which start from the different points $x_0 = 0.1$ and $x_0' = 0.9$, the bifurcation diagrams and Lyapunov exponents.

4. Conclusions

In this paper, a new PRNG based on the composition of the chaotic maps has been proposed. We have proved, using mathematically concepts from discrete dynamical nonlinear systems, that the composition of chaotic maps preserves and, moreover, improves the chaotic behavior of a single map. The experiments have demonstrated a good randomness of the new proposed PRNG. These make them a very good candidate for constructing key streams which can be used in real-time encryption applications.

References

[1] K. Alligood, T. Souer, J. York, "Chaos: an introduction to Dynamical Systems", Springer, 2000.
[2] R. Boriga, A.C. Dascalescu,
[3] S. Katsutra, and W. Fukuda, "Exactly solvable models showing chaotic behavior", Physica 130A:597-605, 1985
[4] L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm," Physics Letters A, vol. 289, pp. 199–206, 2001.
[5] V. Patidar , N. K. Pareek, "A pseudorandom bit based on chaotic logistic map and its statistical testing," Informatica 441–452 441 , 2008.
[6] R. Kadir, M. Maarof, "A Comparative Statistical Analysis of Pseudorandom Bit Sequences", Fifth International Conference on Information Assurance and Security, 2009.
[7] Shujun Li, G. Chen, "On the Security of the Yi-Tan-Siew Chaotic Cipher", IEEE
[8] Li Shujun, M. Xuanqinb, and C Yuanlongc "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher, Institute of Image Processing, School of Electronics and Information Engineering, 2003".
[9] C. I. Rancu, A. Serbanescu "Chaos – Based Cryptography. A solution for information Security", Buletin of the Transilvania University of Brasov, 2009.