Robust PRNG based on homogeneously distributed chaotic dynamics

Oleg Garasym, René Lozi, Ina Taralova

Robust PRNG based on homogeneously distributed chaotic dynamics

Oleg Garasym[1], René Lozi[2] and Ina Taralova[1]

[1]Ecole Centrale de Nantes, France; [2]Laboratoire J. A. Dieudonné, UMR CNRS 7351 Nice Sophia-Antipolis, France

E-mail: oleg.garasym@irccyn.ec-nantes.fr, rlozi@unice.fr and ina.taralova@irccyn.ec-nantes.fr

Abstract. This paper is devoted to the design of new chaotic Pseudo Random Number Generator (CPRNG). Exploring several topologies of network of 1-D coupled chaotic mapping, we focus first on two dimensional networks. Two topologically coupled maps are studied: TTL^{RC} non-alternate, and TTL^{SC} alternate. The primary idea of the novel maps has been based on an original coupling of the tent and logistic maps to achieve excellent random properties and homogeneous /uniform/ density in the phase plane, thus guaranteeing maximum security when used for chaos base cryptography. In this aim two new nonlinear CPRNG: $MTTL_2^{SC}$ and $NTTL_2$ are proposed. The maps successfully passed numerous statistical, graphical and numerical tests, due to proposed ring coupling and injection mechanisms.

1. Introduction

tremendous development of new IT technologies, e-banking, e-purchasing, etc. nowadays increases incessantly the needs for new and more secure cryptosystems. The latter are used for information encryption, pushing forward the demand for more efficient and secure pseudo-random number generators [1]. At the same time, chaotic maps show up as perfect candidates able to generate independent and secure pseudo-random sequences (used as information carriers or directly involved in the process of encryption/decryption). However, the majority of well-known chaotic maps are not naturally suitable for encryption [2] and most of them don't exhibit even satisfactory properties for encryption. Generally, it is known [3] that true randomness is only obtained using a nondeterministic physical process like radioactivity, pseudo-randomness corresponds to a mathematical algorithm satisfying statistical properties and chaos is limited to dynamical systems. Some authors [4] refer flawly to true or truly random numbers while they are involving only chaotic numbers in their articles. True randomness is never reproducible, which forbids the use of true random numbers in cryptographic algorithms which need synchronisation. Electronic circuits cannot be used because small variations in temperature change the characteristic function which models the behavior, therefore it could not be exactly reproduced. Therefore, we deal with pseudo-random number generator (PRNG)and in this aim we propose the original idea to couple tent and logistic map, and to add an injection mechanism to keep bounded the escaping orbits.

In 1973, sir Robert May, a famous biologist introduced the nonlinear, discrete time dynamical system called logistic equation:

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

as a model for the fluctuations in the population of fruit flies in a closed container with constant food [5]. Since that early time this logistic equation has been extensively studied especially by May [6], and Feigenbaum [7] under the equivalent form:

$$x_{n+1} = f_\mu(x_n) \tag{2}$$

where

$$f_\mu(x_n) \equiv L_\mu(x) = 1 - \mu x^2 \tag{3}$$

Another often studied discrete dynamical system is defined by the symmetric tent map:

$$f_\mu(x_n) \equiv T_\mu(x_n) = 1 - \mu|x| \tag{4}$$

In both cases, μ is a control parameter that has impact to chaotic degree, and those mappings are sending the one-dimensional interval $[-1, 1]$ into itself.

Those two maps have also been fully explored with the hope of generating pseudo-random numbers [8]. However the collapsing of iterates of dynamical systems or at least the existence of very short periodic orbits, their non constant invariant measure, and the easily recognized shape of the function in the phase space should lead to avoid the use of such one-dimensional map (logistic, baker, or tent, etc.) or two dimensional map (Hénon, standard or Belykh, etc.) as a pseudo-random number generator (see [9] for a survey). However, the very simple implementation in computer program of chaotic dynamical systems led some authors to use them as a base of cryptosystem [10]. They are topologically conjugate, that means they have similar topological properties (distribution, chaoticity, etc.) however due to the structure of number in computer realization their numerical behavior differs drastically. Therefore the original idea here is to combine features of tent (T_μ) and logistic (L_μ) maps to achieve new map with improved properties, trough combination of several network topologies. In this paper we propose new ideas of tent and logistic maps coupling, based on the analogy between mathematical circuits and electrical circuits [11].

2. Exploring topologies of network of coupled chaotic maps

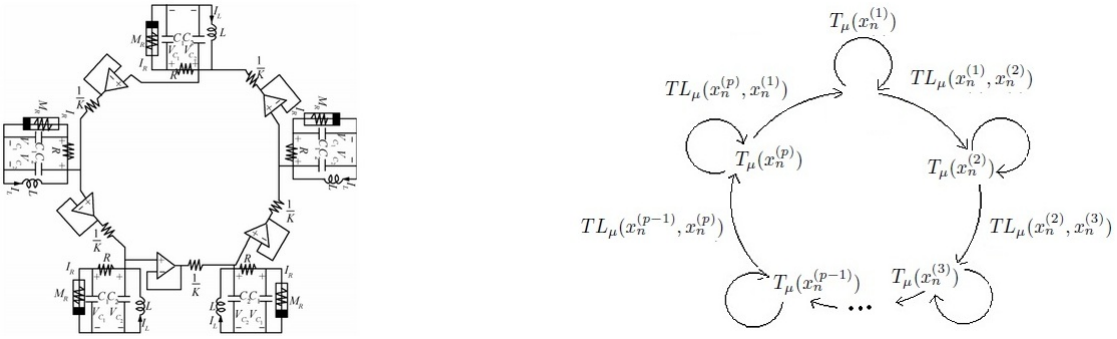
Ring and auto-coupling of chaotic maps (or circuits) enables to combine the individual circuit's dynamics, and therefore, to obtain more complex dynamic behavior. For instance, different ways of coupling several Chua's circuits gives rise to hyperchaos [11]. It should be emphasized that these representations (Fig. 1a) are also a perfect tool to investigate the topology of the map.

Looking at the equations we can inverse the shape of the graph of the tent map T on the step of logistic map L. Thus, our proposition has the form:

$$f_\mu(x) \equiv TL_\mu(x) = \mu|x| - \mu x^2 = \mu(|x| - x^2) \tag{5}$$

Recall that both logistic and tent maps have never been used in cryptography because they have weak security (collapsing effect) [12, 13] if applied alone. Thus, systems are often used in modified form to construct PRNG. The Lozi system [14] provides method to increase randomness properties of the tent map over its coupling. In another way, we propose to couple T_μ map over combination with TL_μ map (5). When used in more than one dimension, TL_μ map can be considered as a two dimensional map:

$$TL_\mu(x^{(1)}, x^{(2)}) = \mu(|x^{(1)}| - (x^{(2)})^2) \tag{6}$$



a) b)

Figure 1. a) Circuits of ultra-weak coupling of chaotic Chua's circuits b) Auto and ring-coupling between states of the M_p)

Hence it is possible to define a mapping M_p from $[-1,1]^p \to [-1,1]^p$

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ T_\mu(x_n^{(p)}) + TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{cases} \tag{7}$$

Note that the system dynamics is unstable and trajectories quickly spread out. Therefore, to solve the problem of holding dynamics in the bound $[-1,1]^p$ the following injection mechanism has to be used:

$$\begin{array}{c} \text{if } x_{n+1}^{(i)} < -1 \\ \text{then add } 2 \\ \text{if } x_{n+1}^{(i)} > 1 \\ \text{then substract } 2 \end{array} \tag{8}$$

in this case for $1 \le i \le p$, points come back from $[-3,3]^p$ to $[-1,1]^p$.

Auto and ring-coupling between states (Fig.1b) of the map and injection mechanism influence the system dynamics making its dynamics complex enough for our application purposes.

Used in conjunction with T_μ the TL_μ function allows to establish mutual influence between system states. The function is attractive because it performs contraction and stretching distance between states improving chaotic distribution. Thus, TL_μ function is a powerful tool to change dynamics.

The coupling of the simple states has excellent effect on chaos achieving, because:

- Simple states interact with global system dynamics, being a part of it.
- The states interaction has a global effect.

Hence, if we use TL_μ to make impact on the dynamics of simple maps, then excellent effect on chaoticity and randomness could be achieved. The proposed function improve the complexity of a simple map.

Note that the system (7) can be seen in the scope of a general point of view, introducing constants k^i which generalize considered topologies. It is called non-alternate if $k^i = +1$, or $k^i = -1$, $1 \le i \le p$, or alternate if $k^i = (-1)^i$, $1 \le i \le p$. It can be a mix of alternate and non-alternate if $k^i = +1$ or -1 randomly. As well it has been already shown that the coupling

could improve the performances of well known chaotic attractors (Chua, Lorenz, Rossler, etc.) for application purposes [11].

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1 \times TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + k^2 \times TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ T_\mu(x_n^{(p)}) + k^p \times TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{cases} \tag{9}$$

In this paper we will discuss only systems exhibiting the best properties for CPRNG. Therefore, we will consider only two 2-D systems: $TTL_\mu^{RC}(x_n^{(2)}, x_n^{(1)})$ **non-alternate**:

$$TTL_\mu^{RC} : \begin{cases} x_{n+1}^{(1)} = 1 - \mu|x_n^{(1)}| + \mu(|x_n^{(2)}| - (x_n^{(1)})^2) \\ x_{n+1}^{(2)} = 1 - \mu|x_n^{(2)}| + \mu(|x_n^{(1)}| - (x_n^{(2)})^2) \end{cases} \tag{10}$$

and $TTL_\mu^{SC}(x_n^{(1)}, x_n^{(2)})$ **alternate**:

$$TTL_\mu^{SC} : \begin{cases} x_{n+1}^{(1)} = 1 - \mu|x_n^{(1)}| - \mu(|x_n^{(1)}| - (x_n^{(2)})^2) \\ x_{n+1}^{(2)} = 1 - \mu|x_n^{(2)}| + \mu(|x_n^{(1)}| - (x_n^{(2)})^2) \end{cases} \tag{11}$$

Here RC stand for ring-coupling and SC for standard coupling.

3. Randomness study of the new maps TTL_μ^{RC} and TTL_μ^{SC}

We are now assessing the randomness of both selected maps. The associated dynamical system is considered to be random and could be applied to cryptosystems if the chaotic generator meets the requirements 1-8 on Fig.2. If one of the criterion is not satisfied, the behavior is less random than expected.

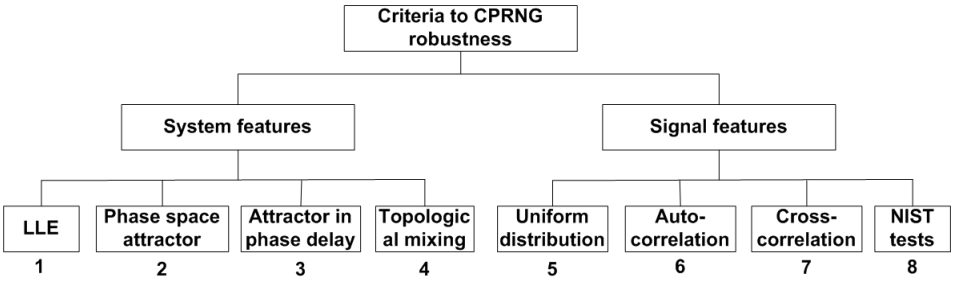


Figure 2. The main criteria for PRNG robustness

As it has been summarized in the scheme (Fig.2) a generator could be taken into consideration for cryptography application if and only if each criterion is satisfied. In the limited extend of this article we give a sketch of the assessment of some criteria such as criteria 1 (Fig. 4), 2 and 5 (Fig. 5, 7), 3 (Fig. 9), 8 (Fig. 12), for criteria 4, 6, 7 one can refer to [15].

Chaotic map behavior primarily depends on the initial guess x_0 and "control" parameter μ. However, the dependence versus the initial guess, x_0 has less importance when the global phase portrait is scrutinized. Thus, to study the dependency of parameter μ a bifurcation diagram is an appropriate tool. To create the diagram for the new map, a particular initial value of x_0 is randomly selected, and the map is iterated for a given μ. A certain number of firstly generated points is cut off to remove the transient part of the iterated points, and the following points are plotted. Afterwards, the process is repeated incrementing slightly μ.

To plot the bifurcation diagram for the 2-D systems TTL_{μ}^{RC} non-alternate (Fig. 3.a) and TTL_{μ}^{SC} alternate (Fig. 3.b), 10,000 iterations have been generated for each initial value and the first 1,000 points have been cut off as transient. Thus, 9,000 points are plotted for each μ parameter. The graphs are the same for $x^{(1)}$ and $x^{(2)}$.

a) b)

Figure 3. Bifurcation diagram of 2-D new maps a) TTL_{μ}^{RC} non-alternate (10) b) TTL_{μ}^{SC} alternate (11)

For both graphs starting from $\mu = 0$ to $\mu = 0.25$, we can observe a period 1 (*i.e.* a fixed point). Then the steady-state response undergoes a so-called pitchfork bifurcation to period 2. Following bifurcation undergoes multiple periods. At higher μ values, the behavior is generally chaotic. However, for TTL_{μ}^{RC} near $\mu = 1.1$ (Fig. 3.a) periodic windows appear. The subsequent intervals show perfect chaotic dynamics.

The Lyapunov exponent (LE) is a measure of the system sensitivity to initial conditions. The function of Lyapunov exponent λ is the characteristic of chaotic behavior in nonlinear maps. If the largest LE $\lambda > 0$ the system exhibits chaotic behavior.

Let us observe the graphics of Lyapunov exponent for TTL_{μ}^{RC} non-alternate (Fig. 4.a) and TTL_{μ}^{SC} alternate (Fig. 4.b) maps. For the plotting $10,000$ iterations were taken into account for every value of μ. The μ parameter is selected from 0.5 to 2. The list of points formed with μ is described on the horizontal coordinate and the measure λ is on the vertical coordinate.

a) b)

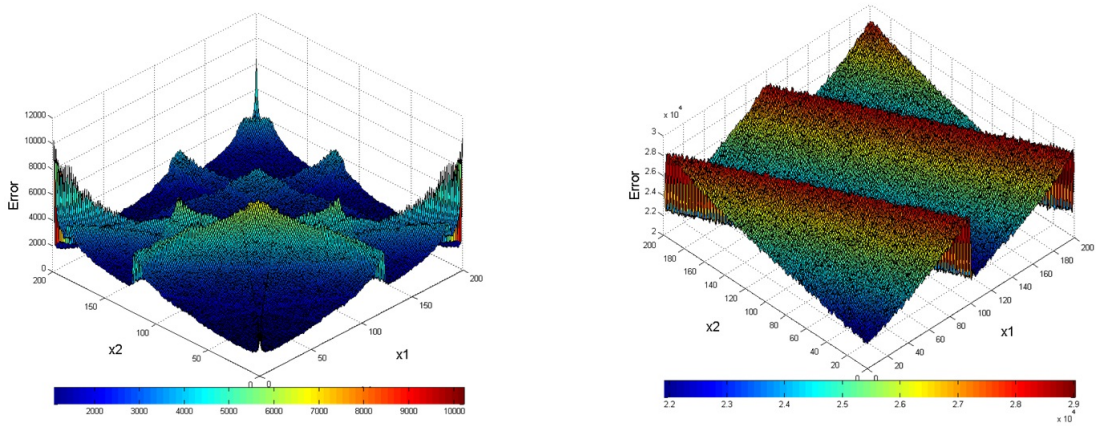
Figure 4. Function of the largest Lyapunov exponent for 2-D new maps a) TTL_{μ}^{RC} non-alternate map (10) b) TTL_{μ}^{SC} alternate map (11)

Graphs of the largest Lyapunov exponent are in exact agreement with those of the bifurcations. The measure λ is positive indicating chaotic dynamics which increases showing the strongest chaos at $\mu = 2$.

The study demonstrates that TTL_{μ}^{RC} non-alternate (Fig. 4.a) and TTL_{μ}^{SC} alternate (Fig. 4.b) maps exhibit the best chaotic behavior characteristics when $\mu = 2$, therefore we will continue our study fixing the parameter to this value. On the graphs for any given initial point x_0

trajectories will look like chaotic. Hence, we can study an attractor in phase space and phase delay.

The quality of the entire cryptosystem [15] mostly depends on PRNG and one of the most important things for robust PRNG is uniform distribution of generated values in the space (Criterion 5, Fig. 2). An approximated invariant measure gives the best description of probability. Thus, the invariant measure [16] is used for precise study of the points distribution. Using the approximate density function the best picture of points density can be achieved. The graph of the function demonstrates distribution comparison between regions. The size of each of the boxes is measured by *step*. In other words the plane is divided $boxes[i, j]$ with square area $step^2$, after counting the points entering into the box $box[i, j]$.



a) b)

Figure 5. Approximate density function, where $step = 0.01$, 10^9 points are generated a) TTL_2^{RC} non-alternate map b) TTL_2^{SC} alternate map

For the approximation function the pattern was divided into 200 boxes or $step = 0.01$, 10^9 points were generated. Note that those values are the maximum possible used to calculate with a laptop computers. The graphs (Figs. 5a and 5b) of the detailed points distribution demonstrates that both systems do not have excellent distribution in phase space. Note: due to the squared nonlinearity of logistic map it is impossible to define explicitly a transition matrix corresponding to a Markov chain of TTL_2^{SC}, therefore it is only possible to compute numerically its invariant measure.

Good results are demonstrated with two different kinds of coupling, simple and ring-coupling in dimension 2, thus increasing the complexity of the system. However as those results are not completely satisfactory, an improved geometry of coupling is introduced allowing us to describe a new 2-D Chaotic Pseudo Random Number Generator (CPRNG). It was noticed that some parts of the graph are perfectly joined, giving us an idea to improve the points density using some correction in the equations.

4. Two new 2-D chaotic PRNG

Considering the results of section 3 it seems possible to improve the randomness of the 2-D topology. First, let us rewrite the mapping TTL_μ^{SC} alternate (11) where $\mu = 2$ as follows:

$$TTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 4|x_n^{(1)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(|x_n^{(1)}| - |x_n^{(2)}|) \end{cases} \tag{12}$$

The first problem is that top green coloured region occurs after injection is applied. Thus, we develop the system (15) in such a way that green coloured region "stays" in such position without injection mechanism. Secondly, we need to reduce the width of the region. Obviously, it is possible to achieve this need by reducing the impact of the state x^1, with the new following map:

$$MTTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 2|x_n^{(1)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(|x_n^{(1)}| - |x_n^{(2)}|) \end{cases} \tag{13}$$

with the injection mechanism (8) used as well, but restricted to 3 phases:

$$\begin{array}{c} if\ x_{n+1}^{(1)} > 1\ then\ substract\ 2 \\ if\ x_{n+1}^{(2)} < -1\ then\ add\ 2 \\ if\ x_{n+1}^{(2)} > 1\ then\ substract\ 2 \end{array} \tag{14}$$

The results of the modifications are demonstrated on Figs. 6, 7.a and 7.b. The injection mechanism in 3 phases (Fig. 6) matches the regions in an excellent way. The techniques used, greatly improve the points density in the phase space (Figs. 7).

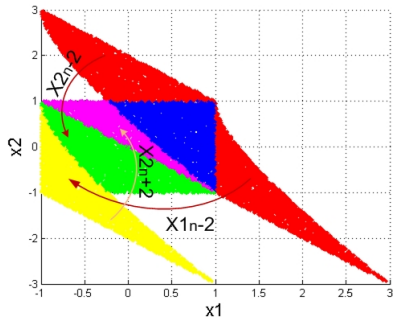


Figure 6. Injection mechanism (14) of $MTTL_2^{SC}$ alternate map

The numerical results of the errors distributions (Fig. 8) shows excellent distribution till 10^9 points which is limited by the classical computer power. Moreover, the largest Lyapunov exponent is equal to 0.5905 indicating strong chaotic behavior.

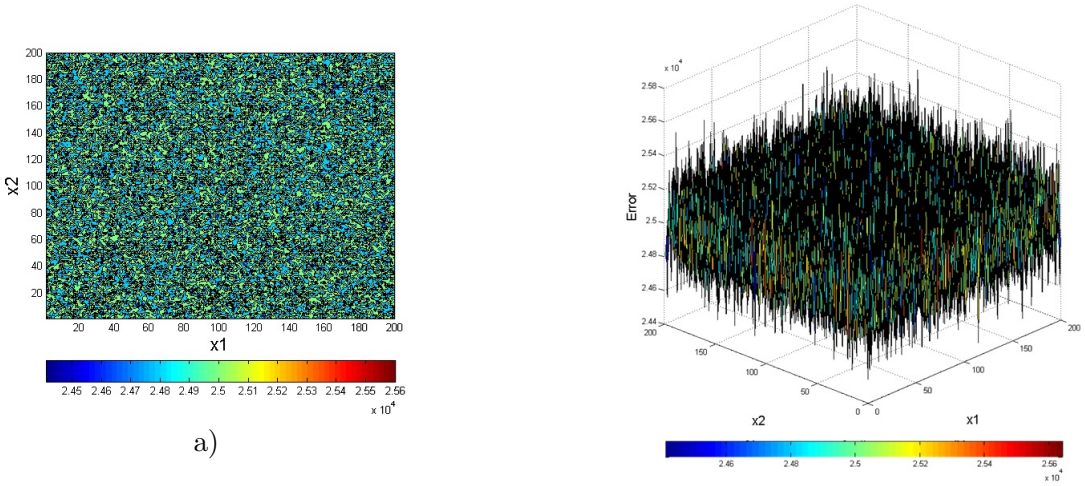
The graph (Fig. 8) shows straight error reducing that proves uniform points distribution when the number of iterates increases.

The points distribution of the attractor in phase delay is quite good as well (Fig. 9), where 10^9 points have been generated. In Fig. (9.b) tent distribution can be recognized for $x^{(2)}$ variable but for encryption we need only output of one state (in our case $x^{(1)}$). Both states make strong impact on each other and for the global dynamics, reaching significant points distribution on the torus and chaoticity.

We introduce now another structurally simple 2-D map using another topology that exhibits homogeneous dynamics distribution in phase space and phase delay space for both states. The map is described as follows:

$$NTTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 - 2|x_n^{(2)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 - 2(|x_n^{(2)}| - |x_n^{(1)}|) \end{cases} \tag{15}$$

applying injection mechanism (Fig. 10) to hold dynamics in $[-1, 1]^2$:



a) b)

Figure 7. Approximate density function of $MTTL_2^{SC}$ alternate map, where $step = 0.01$, 10^9 points are generated a) Boxes method b) 3D

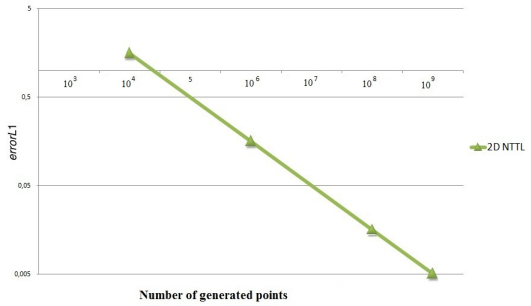
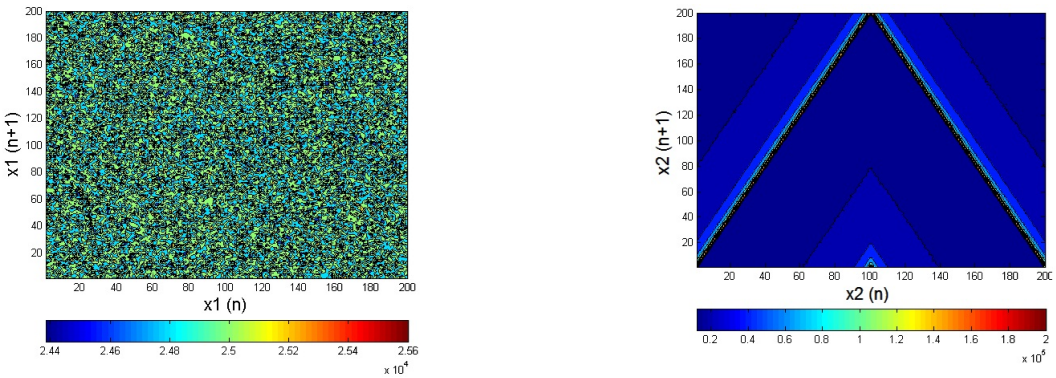


Figure 8. Approximate distribution errors, for the system (13)



a) b)

Figure 9. a) Attractor in the phase delay, 10^9 points are generated, for the system (13) a) $(x_n^{(1)}, x_{n+1}^{(1)})$ b) $(x_n^{(2)}, x_{n+1}^{(2)})$

$$\begin{array}{c} if\ x_{n+1}^{(2)} < -1 \text{ then add } 2 \\ if\ x_{n+1}^{(2)} > 1 \text{ then substract } 2 \end{array} \tag{16}$$

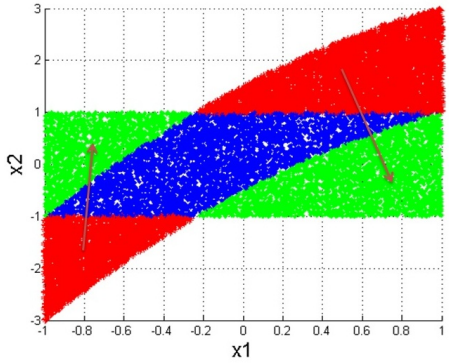
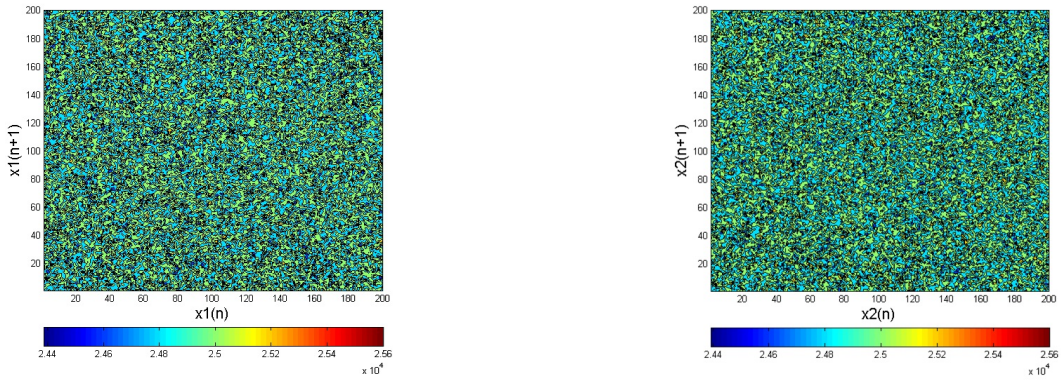


Figure 10. Injection mechanism (14) of $NTTL_2$ alternate map

The $NTTL_2$ exhibits excellent density in phase delay for both states x^1 and x^2 (Fig. 11) and successfully passed all criteria (Fig. 2), being very promising for real application.



a) b)

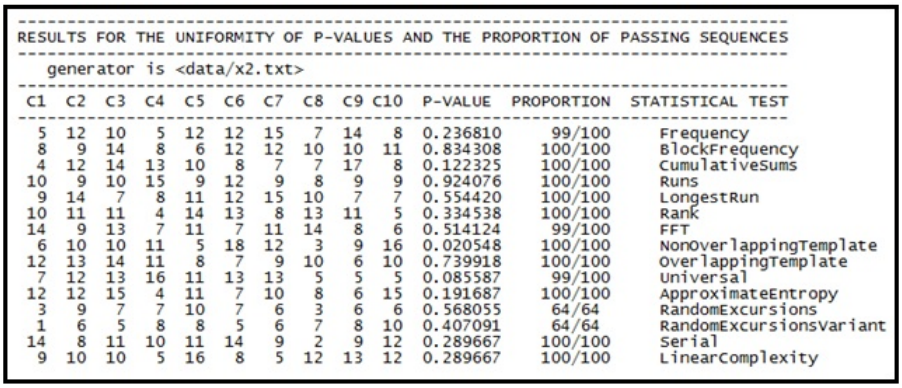
Figure 11. $NTTL_2$ density in phase delay **a)** $(x_n^{(1)}, x_{n+1}^{(1)})$ **b)** $(x_n^{(2)}, x_{n+1}^{(2)})$

The $NTTL_2$ map exhibits complex dynamics capable to refuse statistical attacks since it successfully passed NIST tests (Fig. 12).

The future work will be devoted to the investigation of topologies in 3 dimensional space where the complexity of dynamical phenomena is expected to exhibit even better performances, though being more intricate [17]

5. Conclusion

In this paper we have proposed the original idea to couple two well-known chaotic maps (tent and logistic one), which considered separately - do not exhibit the required features for encryption purposes because they have weak security (collapsing effect) when applied alone. The new coupling changed qualitatively the overall system behavior, because the maps used with injection mechanism and coupling between states increased their complexity.



RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/x2.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
5	12	10	5	12	12	15	7	14	8	0.236810	99/100	Frequency
8	9	14	8	6	12	12	10	10	11	0.834308	100/100	BlockFrequency
4	12	14	13	10	8	7	7	17	8	0.122325	100/100	CumulativeSums
10	9	10	15	9	12	9	8	9	9	0.924076	100/100	Runs
9	14	7	8	11	12	15	10	7	7	0.554420	100/100	LongestRun
10	11	11	4	14	13	8	13	11	5	0.334538	100/100	Rank
14	9	13	7	11	7	11	14	8	6	0.514124	99/100	FFT
6	10	10	11	5	18	12	3	9	16	0.020548	100/100	NonOverlappingTemplate
12	13	14	11	8	7	9	10	6	10	0.739918	100/100	OverlappingTemplate
7	12	13	16	11	13	13	5	5	5	0.085587	99/100	Universal
12	12	15	4	11	7	10	8	6	15	0.191687	100/100	ApproximateEntropy
3	9	7	7	10	7	6	3	6	6	0.568055	64/64	RandomExcursions
1	6	5	8	8	5	6	7	8	10	0.407091	64/64	RandomExcursionsVariant
14	8	11	10	11	14	9	2	9	12	0.289667	100/100	Serial
9	10	10	5	16	8	5	12	13	12	0.289667	100/100	LinearComplexity

a)

Figure 12. $NTTL_2$ map successfully passed NIST tests

We have explored several topologies and finally proposed two new 2-D CPRNG. The proposed models with injection mechanism allow to puzzle perfectly the pieces of the chaotic attractor, like a true random generator. To achieve the best distribution in the phase space, the modified form $MTTL_2^{SC}$ alternate map has been proposed. The new map exhibits excellent features due to the injection mechanism and enables the uniform density in the state space. The system exhibits strong nonlinear dynamics, demonstrating strong sensitivity to initial conditions. It generates an infinite range of intensive chaotic behavior with large positive Lyapunov exponent values. Moreover, $MTTL_2^{SC}$ successfully passed all required tests: cross-correlation, autocorrelation, LLE, NIST tests, uniform attractor on the phase space and phase delay. The system analysis and the dynamics evolution by bifurcation diagram and topological mixing proved the complex behavior. The system orbits exhibited complex behavior with perfect mixing. The study demonstrated totally unpredictable (for any intruder) dynamics making the system strong-potential candidate for high-security applications. Another CPRNG candidate based on $NTTL_2^{SC}$ map was proposed that successfully passed all required statistical, graphical and numerical results for both states components. The $NTTL_2^{SC}$ map demonstrates complex dynamics being very promising to real scale cryptography application.

References

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

[2] Li, C. Y., Chen, Y. H., Chang, T. Y., Deng, L. Y., and To, K. (2012). Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, **20(2)**, 385-389.

[3] Lozi, R. (2012). Emergence of randomness from chaos, *International Journal of Bifurcation and Chaos*, **22 (02)**, 12500211/15.

[4] Nejati, H., Beirami, A., and Massoud, Y. (2008, August). A realizable modified tent map for true random number generation. *In Circuits and Systems*, MWSCAS 2008. 51st Midwest Symposium on (pp. 621-624). IEEE.

[5] May, R. M. (2001). *Stability and complexity in model ecosystems.* Princeton University Press, **Vol. 6**.

[6] May, R. M. (1974). Biological populations with nonoverlapping generations: stable points, stable cycles, and chaos. *Science*, **186(4164)**, 645-647.

[7] Feigenbaum, M. J. (1979). The universal metric properties of nonlinear transformations. *Journal of Statistical Physics*, **21(6)**, 669-706.

[8] Sudret, B. (2008). Global sensitivity analysis using polynomial chaos expansions. *Reliability Engineering and System Safety*, **93(7)**, 964-979.

[9] Lozi, R. (2013) Can we trust in numerical computations of chaotic solutions of dynamical systems? *In Topology and Dynamics of Chaos, Ch. Letellier, R. Gilmore (Eds.)*, World Scientific Series in Nonlinear Science Series A, Chapt. **3**, 2013.

[10] Ariffin, M. R. K., and Noorani, M. S. M. (2008). Modified Baptista type chaotic cryptosystem via matrix secret key. *Physics Letters A*, **372(33)**, 5427-5430.

[11] Lozi, R. (2013) Designing chaotic mathematical circuits for solving practical problems, *International Journal of Automation and Computing*, **vol. 11**, no. 6, pp. 588597, 2014.

[12] Yuan, G., and Yorke, J. A. (2000). Collapsing of chaos in one dimensional maps. *Physica D: Nonlinear Phenomena*, **136(1)**, 18-30.

[13] Lanford III, O. E. (1998). Informal remarks on the orbit structure of discrete approximations to chaotic maps. *Experimental Mathematics*, **7(4)**, 317-324.

[14] Rojas, A. E., Taralova, I., and Lozi, R. (2013). New alternate ring-coupled map for multi-random number generation, *Journal of Nonlinear Systems and Applications*, **4(1)**, 64-69.

[15] Garasym O. (2015). Application of nonlinear dynamics to the design of robust chaotic generators. *PhD thesis, Ecole Centrale de Nantes*, pp. 1-170.

[16] Lozi, R. (2009) Chaotic pseudo random number generators via ultra weak coupling of chaotic maps and double threshold sampling sequences *In proceedings of: ICCSA 2009 The 3rd International Conference on Complex Systems and Applications, University of Le Havre, France*, 20-24.

[17] Manjunath, G., Fournier-Prunaret, D., and Taha, A. K. (2008). A 3-dimensional piecewise affine map used as a chaotic generator *European Conference on Iteration Theory September(ECIT), Yalta, Ukraine*, pp. 7-13.