New nonlinear CPRNG based on tent and logistic maps

Oleg Garasym, Ina Taralova, René Lozi

Author name(s)

Book title

– Monograph –

July 1, 2015

Springer

Contents

Chapter 1
New nonlinear CPRNG based on tent and logistic maps

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 coupled maps are studied: TTL^{RC} non-alternative, and TTL^{SC} alternative. 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 a new nonlinear CPRNG: $MTTL_2^{SC}$ is proposed. In addition, we explore higher dimension and the proposed ring coupling with injection mechanism enables us to achieve the strongest security requirements.

1.1 Introduction

The 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 [**?**]. 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 [**?**] and most of them don't exhibit even satisfactory properties for encryption. To deal with this open problem, we propose the revolutionary idea to couple tent and logistic map, and to add an injection mechanism to bound the escaping orbits. 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).

The various choice of the PRNG and crypto algorithms is necessary to provide continuous, reliable security system. We describe a software approach because it is easy to change cryptosystem to support protection whereas hardware requires more time and big expenses. For instance, after the secure software application called Wi-Fi Protected Access (WPA) protocol have been broken it was simply updated and no expensive hardware needed to be bought.

In the history, there are periods of popular algorithms, cryptographic methods and approaches until the moment they are broken. It is a usual thing in information security one algorithm replaces another because information technologies and mathematics make progress. The one of today's open mathematical problem is factoring the product of two large prime numbers which is foundation for RSA algorithm. The RSA was created by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 and since that time was implemented in widespread applications, is used for an independent cryptographic production [**?**]. Open coding based on the RSA algorithm is utilized in popular encryption package PGP, operating system Windows, various Internet browsers, banking computer systems. Moreover, there exist various international standards for public key cryptography and digital signatures. However, we expect the new cryptographical standards soon, because there are several evidences of weakness of those methods. Recently was known about a "back-door" in PRNG (Dual EC DRBG) which is implemented in RSA algorithm by default.

The second reason is that modern mathematical technology could give a possibility to break the process of obtaining cryptographic keys. In addition, there are many hackers attacks to RSA encryption, thus it could be broken in the nearest future.

Moreover, there is another important problem to be solved. RSA is a public keys system that is much simpler than a system with private keys such as: René Lozi and Estelle Cherrier [**?**], Safwan El Assad [**?**], Singh Ajit and Gilhotra Rimple [**?**].

Consequently, it is necessary to have an alternative way of secure information transmission. Chaos based methods are very promising for application in information security. One of the evidences is that needs for data protection are increased and encryption procedures requires to generate pseudo-random sequences with very long periods. The chaotic maps when used in stirling way could generate not only chaotic number but also pseudo-random numbers as we will show here.

Methods of nonlinear dynamics allow to create with relatively little effort a fundamentally new type of behavior, capable of holding, encrypting and process given information. Foundations of it are that chaotic attractors could contain an infinite set of unstable periodic behaviors. Nowadays there are different ways of chaos application to design symmetric and asymmetric cryptosystems. The methods based on circuits synchronization have been applied to numerous chaotic systems [**?**, **?**]. Nonlinear dynamics is a promising direction to solve the problem of information processing and organization of secure information transmission through the use of systems exhibiting chaotic dynamics.

Here we represent an original idea combining of tent and logistic maps for new chaotic PRNG design. Since, it is a very responsible and challenging task to design CPRNG applicable to cryptography, numerous analysis have been fulfilled. Essentially we focus on 2-D map as a more difficult task achieving excellent chaotic and

randomness properties. The 3-steps injection mechanism, ring- and auto-coupling techniques are used to achieve complex and uniform dynamics. We demonstrate excellently puzzled chaotic dynamics in the space exhibiting sufficient randomness properties only for 2-D map. The most significant tests were successfully passed. Moreover, higher dimensional system here proposed as well. The systems provide also good candidates for CPRNG.

1.2 CPRNG indistinguishable from random

Let us consider a CPRNG that produces binary bits $G : K \to \{0,1\}^n$, where K belongs to keyspace $\mathbb{A}$, n is a number of bits. In real life, for any given $K \in \mathbb{A}$ intruder should not distinguish it from random. Usually, statistical tests are used to the binary sequence analysis. The results could disclose some weakness in generated random sequences or at least refuse the truly random nature of the generator. Whereas statistical tests prove the behavior of the generator as being like truly random, which implies robustness against attacks based on such kind of analysis.

The statistical test is an algorithm that takes its inputs and as an output gives 0 or 1. The given sequence is supposed to be not random whereas output equals 0. In opposite case, where output equals 1 we assume that the given input is random, according to the test. All statistical tests are used to determine either the given sequence that produced by some generator $G(K)$ looks random or it does not look random. However, the well-known fact is when statistical test could make the wrong decision relatively to the sequence [**?**]. Therefore, it is preferable to define PRNG advantage [**?**].

The generator G exhibits weakness if the statistical test Υ was able to distinguish the output from random. However, if the advantage is close to zero $Adv \neq 0$ then the pseudo-random inputs have the same behavior as truly random within statistical test Υ. Therefore, Υ could not distinguish the generator from random.

Generator $G : K \to \{0,1\}^n$ is a secure PRNG if for every efficient statistical tests $\Upsilon : Adv_{PRNG}[\Upsilon, G]$ is negligible or the statistical tests cannot distinguish its output from random.

There are hundreds of statistical tests that confirm or refuse randomness. When for all the tests a given string looks like random, the generator is considered as robust. Due to the tests it will not be able to use statistical attacks on the algorithm if intruder cannot distinguish PRNG from truly random.

Chaotic functions deal with floating points, thus statistical tests are not directly efficient to define if a CPRNG is robust or not. The laws and standards for binary strings cannot fully guarantee robustness since the nature is different. Chaotic PRNG can be used in appearance of noise e.g. in the CSK, CMA, CMI models or as binary string in XOR-function. Therefore, there are more requirements to CPRNG to prove indistinguishability from truly random generator. Note that, today there is no standards on CPRNG analysis, but the primary tests are described in the next section.

1.2.1 Some tests for robustness

There are no standards of security verification, making it difficult to determine whether the system is truly secure. This is the crucial reason why chaos is till not officially used in cryptography. However we represent the main and the most important security tests to chaotic systems.

Progress has been made to the point that chaos can be applied to secure communication [**?**, **?**] and many papers focused on robust chaotic generator design [**?**, **?**, **?**]. There are several criteria respected by the community to the chaotic generators: Largest Lyapunov exponent [**?**], Chaotic attractor in the phase space [**?**, **?**], phase delay [**?**, **?**], Topological mixing [**?**, **?**], Reactivity to small changes in initial conditions (chaotic sensitivity) [**?**, **?**], Uniform distribution [**?**, **?**], Autocorrelation [**?**, **?**], Crosscorrelation [**?**], NIST tests [**?**, **?**].

To prove robustness and ability to cryptosystems applications the chaotic system should demonstrate excellent randomness and chaoticity results. Even if there is no exact and unique chaos definition, the system is considered to be chaotic and could be applied to cryptosystems when the chaotic generator behaves as a performed PRNG (generated sequences must all be unitarily independent etc.). Therefore the following requirements should be fulfilled [**?**]:

- Random pattern : passes statistical tests of randomness;
- Long period : goes as long as possible before repeating;
- Efficiency : executes rapidly and requires little storage;
- Repeatability : produces same sequence if started with same initial conditions;
- Portability : runs on different kinds of computers and is capable of producing same sequence on each.

Therefore, for chaotic PRNG we use the following test: Largest Lyapunov exponent, autocorrelation, cross-correlation, test for uniform distribution, chaotic attractor in phase space and phase delay and finally NIST tests.

1.2.2 Uniform distribution.

Randomness is often associated with unpredictability. However, it is difficult to say if a sequence is predictable or no, thus it is considered as unpredictable if each of the points on the range interval has equal chance to be chosen. The test of uniform distribution gives the answer about probability of the points choice. If all points have equal probability then the chance to predict the next point is very small. Thus, this test is important to analyse whether the sequence is unpredictable.

An excellent PRNG looks like truly random, means unpredictable or there are any correlation between points that have equal chance to be chosen. If the generator is capable to produce the sequences uniformly distributed in phase space and phase delay then the system behavior is like truly random.

There are different tools to analyse points distribution i.e histogram, cumulative distribution. However they give very general information. In order to assess numerical computations more accurately and to qualitatively study the chaotic systems an approximation density function [**?**] is preferable. The approximation $P_{M,N}(x)$ is defined of the invariant measure (the probability distribution function) linked to the 1-dimensional map f going from the interval $J \subset \mathbb{R}$ into itself, when computed with floating numbers. The regular partition of M small intervals (boxes) r_i of J is defined by

$$s_i = -1 + \frac{2i}{M}, i = 0, M \tag{1.1}$$

$$r_i = [s_i, s_{i+1}[\quad i = 0,\ M-2 \ \textit{and}\ r_{M-1} = [s_{M-1}, 1] \tag{1.2}$$

the length of each box is equal to $\frac{2}{M}$ and the r_i intervals form a partition of the interval J

$$J = \bigcup_{0}^{M-1} r_i \tag{1.3}$$

All iterates $f^{(n)}(x)$ belonging to these boxes are collected, after a transient regime of Q iterations decided *a priori*, (i.e. the first Q iterates are neglected). Once the computation of $N+Q$ iterates is completed, the relative number of iterates with respect to N/M in each box r_i represents the value $P_N(s_i)$. The approximated $P_N(x)$ defined is then a step function, with M steps. As M may vary, it is defined by

$$P_{M,N}(s_i) = \frac{M}{N}(\sharp r_i) \tag{1.4}$$

where $\sharp r_i$ is the number of iterates belonging to the interval r_i. $P_{M,N}(x)$ is normalized to 2 on the interval $J = [-1, 1]$.

$$P_{M,N}(x) = P_{M,N}(s_i), \forall x \in r_i \tag{1.5}$$

If the chaotic system is combined of p-coupled maps, then it is important to analyse distribution of each component $x^1, x^2, x_1^2, ..., x^p$ of X and variable X itself in J^p as well. The approximated probability distribution function , $P_{M,N}(x^j)$ associated to one among several components of $F(X)$. It is used equally N_{disc} for M and N_{iter} for N, when they are more explicit.

The discrepancies E_1 (in norm L_1), E_2(in norm L_2) and E_∞ (in norm L_∞) between $P_{N_{disc},N_{iter}}(x^j)$ and the Lebesgue measure, which is the invariant measure are defined by

$$E_{1,N_{disc},N_{iter}}(x^j) = \|P_{N_{disc},N_{iter}}(x^j) - 1\|_{L_1} \tag{1.6}$$

$$E_{2,N_{disc},N_{iter}}(x^j) = \|P_{N_{disc},N_{iter}}(x^j) - 1\|_{L_2} \tag{1.7}$$

$$E_{\infty,N_{disc},N_{iter}}(x^j) = \|P_{N_{disc},N_{iter}}(x^j) - 1\|_{L_\infty} \tag{1.8}$$

The numerical calculation of the uniform distribution allows us to judge about system unpredictability.

1.2.3 NIST tests.

Currently, NIST (National Institute of Standard and Technology) tests are the most powerful and widely used tool to test the sequences for randomness [**?**]. The standard includes 15 tests which on output give 188 results. The methodology allows with hight probability to make conclusion about existing randomness in the sequences. According to the NIST tests the sequences are analysed as follow:

1 Zero hypothesis H_0 is putting forward. The sumption that the given binary sequence is random.
2 Statistic is calculated.
3 The probability value $P \in [0,1]$ is calculated.
4 The probability value P is compared with significance level α, $\alpha \in [0.001;0.01]$. If $P \geq \alpha$ then the hypothesis is accepted, otherwise another hypothesis is taken.

The results of the tested sequence take form of probability vector $P = \{P_1, P_2, \ldots, P_{188}\}$. The P_i test indicates the weakness of the sequence. The standard recommends the sequence of 100 blocks per 10^6 bits. Thus, the sequence length should be equal to 10^8 bits. Each of the given 100 blocks passes the analysis. The testing results are consolidated to the summarised table when in front of the each test there is for example the value 97/100, that means that 97 is the number of blocks that successfully passed the test out of 100. The threshold of fail blocks are 3.

1.3 Exploring topologies of network of coupled chaotic maps

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

$$x_{n+1} = rx_n(1 - x_n) \tag{1.9}$$

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

$$x_{n+1} = f_\mu(x_n) \tag{1.10}$$

where

$$f_\mu(x_n) \equiv L_\mu(x) = 1 - \mu x^2 \tag{1.11}$$

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

$$f_\mu \equiv T_\mu = 1 - \mu|x| \tag{1.12}$$

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 in the hope of generating pseudo-random number easily [**?**]. 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 should 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 [**?**] for a survey). However, the very simple implementation in computer program of chaotic dynamical systems led some authors to use it as a base of cryptosystem [**?**, **?**]. 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 behaviour 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 in several topologies of network.

Looking to 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:

$$f_\mu(x) \equiv TL_\mu(x) = \mu|x| - \mu x^2 = \mu(|x| - x^2) \tag{1.13}$$

Recall that both logistic and tent maps are never used in cryptography because they have weak security (collapsing effect) [**?**, **?**] if applied alone. Thus, systems are often used in modified form to construct PRNG [**?**, **?**]. The Lozi system [**?**] 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 (**??**). When used in more than one dimension, TL_μ map can be considered as a two variable map:

$$TL_\mu(x^{(1)}, x^{(2)}) = \mu(|x^{(1)}| - (x^{(2)})^2) \tag{1.14}$$

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

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ T_\mu(x_n^{(p)}) + TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{cases} \tag{1.15}$$

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:

$$\begin{array}{c} if\ x_{n+1}^{(i)} < -1 \\ then\ add\ 2 \\ if\ x_{n+1}^{(i)} > 1 \\ then\ substract\ 2 \end{array} \tag{1.16}$$

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

Used in conjunction with $T_\mu$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 the global effect.

Hence, if we use TL_μ to make impact on dynamics of the simple maps then excellent effect on chaoticity and randomness could be achieved. The proposed function improve complexity of a simple map. The question is how to study the received system. Poincaré was one of the first who used graphical analysis of the complex systems. We will use also graphical approach to study new chaotic systems, but not only, other theoretical assessing functions are involved in our study.

Note that the system (**??**) can be seen in the scope of a general point of view, introducing constants k^i which generalize considered topologies. It is called alternative if $k^i = +1$, $1 \leq i \leq p$, or non-alternative if $k^i = +1$, $1 \leq i \leq p$; or $k^i = -1$, $1 \leq i \leq p$. It can be a mix of alternative and non-alternative if $k^i = +1$ or -1 randomly.

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1 \times TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + k^2 \times TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ T_\mu(x_n^{(p)}) + k^p \times TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{cases} \tag{1.17}$$

In this paper we will discuss only systems exhibiting the best properties for CPRNG.

1.3.1 2-D topologies

The initial purpose of new CPRNG design was to obtain excellent uniform distribution, successfully passing randomness and chaoticity tests. Thus we propose to consider firstly two 2-D models: alternative ($k^1 = -1$, $k^2 = 1$) and non-alternative ($k^1 = k^2 = 1$). However, coupling between states by TL_μ can be made in different ways:

1 Ring coupling with two choices:

$$TL_\mu^{RC}(x^{(1)},x^{(2)}) = \begin{cases} T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \\ T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \end{cases} \tag{1.18}$$

or

$$TL_\mu^{RC}(x^{(2)},x^{(1)}) = \begin{cases} T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \\ T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \end{cases} \tag{1.19}$$

2 Simple coupling with also two choices:

$$TL_\mu^{SC}(x^{(1)},x^{(2)}) = \begin{cases} T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \\ T_\mu(x^{(1)}) - L_\mu(x^{(2)}) \end{cases} \tag{1.20}$$

or

$$TL_\mu^{SC}(x^{(2)},x^{(1)}) = \begin{cases} T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \\ T_\mu(x^{(2)}) - L_\mu(x^{(1)}) \end{cases} \tag{1.21}$$

The general form of the new 2-D map we consider is as follow:

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1 \times TL_\mu((x^{(i)},x^{(j)})) \\ T_\mu(x_n^{(2)}) + k^2 \times TL_\mu((x^{(i')},x^{(j')})) \end{cases}$$

with $i, j, i', j' = 1$ or 2 and TL_μ being either TL_μ^{RC} or TL_μ^{SC}. *Remark:* Ring-coupling can be expected to higher dimensions but not the single case because we obtain the same expression of the function.

However, it is undesirable to use $TL_\mu^{SC}(x^{(1)},x^{(2)})$ because (**??**) implies

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1(T_\mu(x_n^{(1)}) - L_\mu(x_n^{(2)})) \\ T_\mu(x_n^{(2)}) + k^2(T_\mu(x_n^{(1)}) - L_\mu(x_n^{(2)})) \end{cases}$$
$$\Leftrightarrow \begin{cases} x_{n+1}^{(1)} = k^1 L_\mu(x_n^{(2)}) \\ x_{n+1}^{(2)} = k^2 L_\mu(x_n^{(2)}) \end{cases}$$

which is trivial.

If one uses $TL_{\mu}^{RC}(x^{(2)},x^{(1)})$ alternative system then one of the states will have more "power" than another one, loosing good distribution of points property. For the same reason $TL_{\mu}^{SC}(x^{(1)},x^{(2)})$ or $TL_{\mu}^{SC}(x^{(2)},x^{(1)})$ non-alternative ($k=1$) and $TL_{\mu}^{SC}(x^{(2)},x^{(1)})$ alternative are not recommended to use.

Therefore, we will consider only two 2-D systems: $TTL_{\mu}^{RC}(x_n^{(2)})$ **non-alternative**:

$$TTL_{\mu}^{RC}: \begin{cases} x_{n+1}^{(1)} = 1-\mu|x_n^{(1)}|+\mu(|x_n^{(2)}|-(x_n^{(1)})^2) \\ x_{n+1}^{(2)} = 1-\mu|x_n^{(2)}|+\mu(|x_n^{(1)}|-(x_n^{(2)})^2) \end{cases} \tag{1.22}$$

and $TTL_{\mu}^{SC}(x,y)$ **alternative**:

$$TTL_{\mu}^{SC}: \begin{cases} x_{n+1}^{(1)} = 1-\mu|x_n^{(1)}|-\mu(|x_n^{(1)}|-(x_n^{(2)})^2) \\ x_{n+1}^{(2)} = 1-\mu|x_n^{(2)}|+\mu(|x_n^{(1)}|-(x_n^{(2)})^2) \end{cases} \tag{1.23}$$

Both systems were selected because they have balanced contraction and stretching process between states allowing to achieve uniform distribution of the chaotic dynamic.

1.3.2 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.**??** which are described in Sec.1.3. If one of the criterion is not satisfied the behavior is less random than expected.

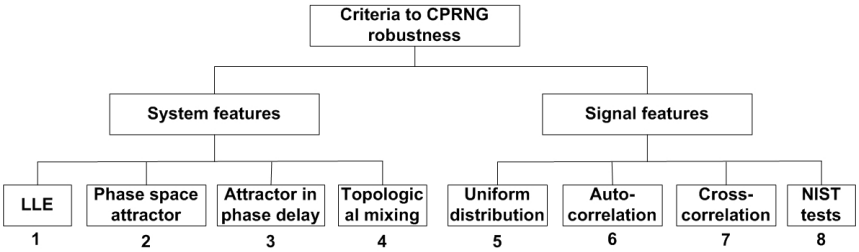


Fig. 1.1 The main criteria for PRNG robustness

As it has been summarized in the scheme (Fig.**??**) a generator could be taken into consideration for cryptography application if and only if every criterion is satisfied.

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-alternative (Fig. **??**) and TTL_{μ}^{SC} alternative (Fig. **??**), 10,000 iterations are generated for each initial value and the first 1000 points are cut off as transient. Thus, 9,000 points are plotted for each μ parameter. The graphs are the same for $x^{(1)}$ and $x^{(2)}$.

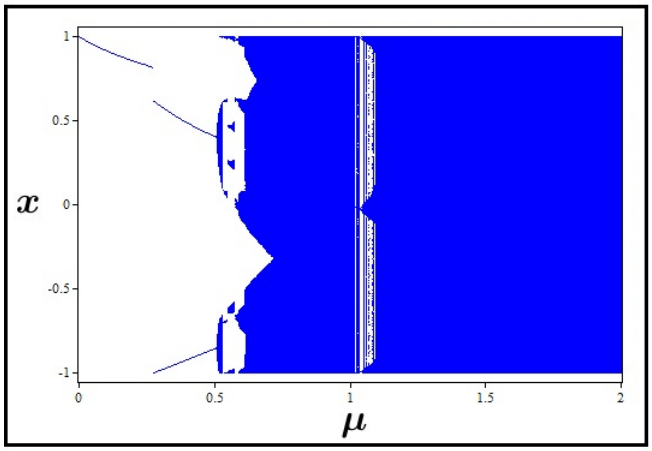


Fig. 1.2 Bifurcation diagram of 2-D new map: TTL_{μ}^{RC} non-alternative (**??**)

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. **??**) periodic windows appear. The subsequent intervals show perfect chaotic dynamics.

Bifurcation diagrams are very useful analysis tools for studying the behavior of nonlinear maps as well as control parameters impact on the dynamic. A complementary study of chaos is the graph of Lyapunov exponent.

The Lyapunov exponent 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 $\lambda > 0$ the system exhibits chaotic behaviour.

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

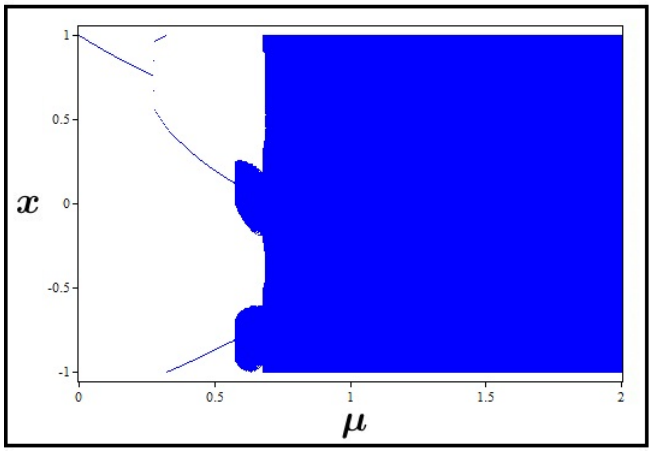


Fig. 1.3 Bifurcation diagram of 2-D new map: TTL_{μ}^{SC} alternative (**??**)

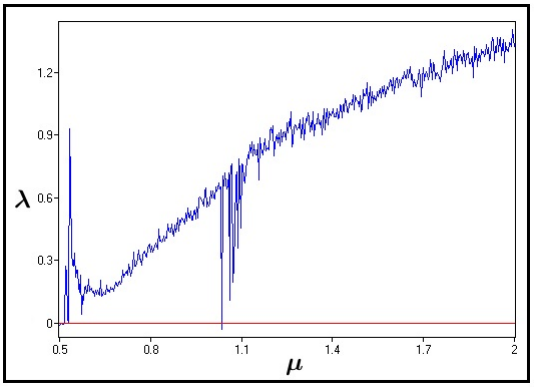


Fig. 1.4 Largest Lyapunov exponent for 2-D TTL_{μ}^{RC} non-alternative map (**??**)

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

The study demonstrates that TTL_{μ}^{RC} non-alternative (Fig. **??**) and TTL_{μ}^{SC} alternative (Fig. **??**) maps exhibit the best chaotic behavior characteristic 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.

Let us plot the attractor in phase space: $x_n^{(1)}$ versus $x_n^{(2)}$ to analyse the points distribution. Observing graphs of chaotic attractor we can make decision about complexity, notice weakness or infer the randomness nature. To plot the attractor 3×10^4 points have been generated, 10^4 points of the transient regime have been cut off.

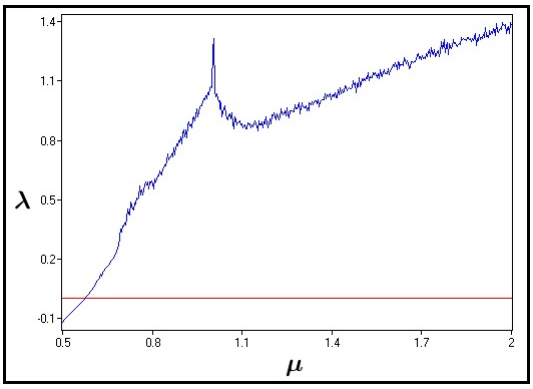


Fig. 1.5 Largest Lyapunov exponent for 2-D TTL_{μ}^{SC} alternative map (**??**)

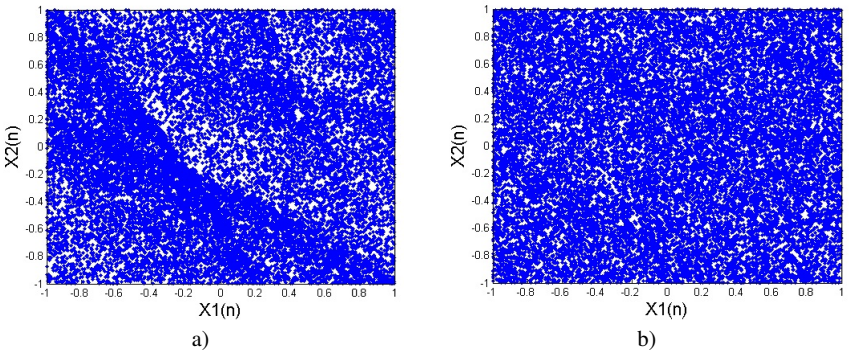


Fig. 1.6 Phase space attractor of 2-D new maps, 2×10^4 points are generated a) TTL_2^{RC} non-alternative (**??**) b) TTL_2^{SC} alternative (**??**)

The graphs of the attractor in phase space for TTL_2^{RC} non-alternative (Fig. **??**a) and TTL_2^{SC} alternative (Fig. **??**b) maps are quite different. The first one has well scattered points on all the pattern, but there are some more "concentrated" regions forming curves on the graph. We will search answer to the questions: "Why there are more concentrated regions? From where curves creates?", by considering the injection mechanism.

Without this mechanism dynamics goes out of the square $[-1,1]^2$ (Fig. **??**a). The maximal distance that points are reaching is 3 and the minimal is -3. Thus, equations (**??**) are preserved, however their influence to the dynamics is different versus the Lozi system [**?**]. For the plotting, 2×10^4 points have been generated, 77 % of the points are scattered out of the $[-1,1]^2$. The mechanism consists of p-steps for a p-dimensional system in each step the value 2 is added or subtracted to the variables if the dynamics goes out of the bounds (**??**). On the first step 69 % points are injected to the interval (Fig. **??**.b) after passing second injection step (Fig. **??**.c) all points are driven base to the square $[-1,1]^2$ (Fig. **??**.d). Therefore mechanism adds non-

linearity and complexity to the system which is an advantage from the security point of view, in the case of cryptographic use.

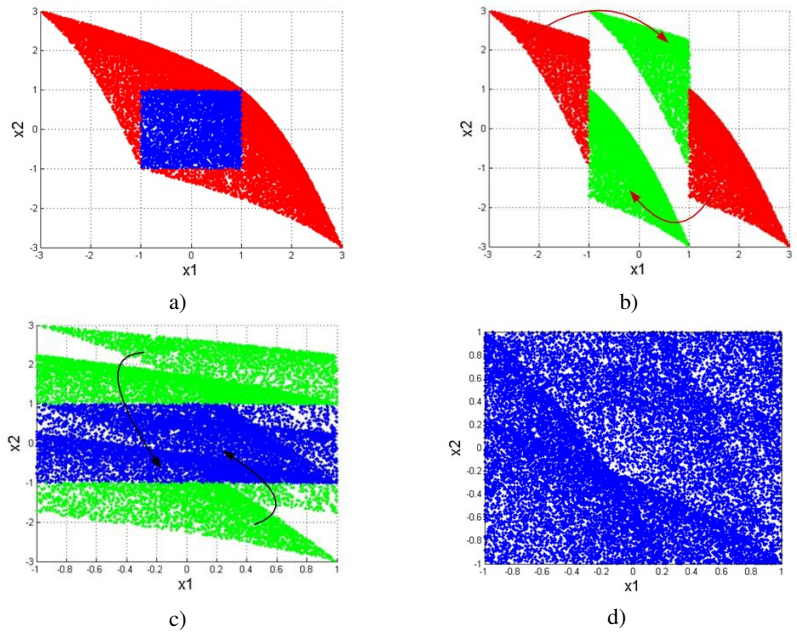


Fig. 1.7 Injection mechanism $[-3,3]^2 \Rightarrow [-1,1]^2$ for TTL_2^{RC} non-alternative map **a)** 2-D chaotic map without adding / substruction **b)** injection $x_n^{(1)}$ to the torus $[-1,1]^2$ **c)** injection $x_n^{(2)}$ to the torus $[-1,1]^2$ **d)** results after passing injection mechanism

The graphs of the attractor in phase space for TTL_2^{SC} alternative map looks uniformly distributed on the plain pattern without any visible concentrated regions (**??**.b.). The injection mechanism impact on the points distribution is given on the Fig. **??**

The quality of the entire cryptosystem 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. **??**). An approximated invariant measure gives the best picture of probability. Thus, the invariant measure (**??**) 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 demonstrate distribution comparison between regions. The size of each of the boxes is measured by $step$. In other words the plain is divided $boxes[i,j]$ with square $step^2$ after the counts the number of points enter into the box $box[i,j]$ is counted.

For the approximation function the pattern was divided for 200 boxes or $step = 0.01$, 10^9 points were generated. Note that those values are the maximal possible used to calculate with a laptop computers. The graphs (Figs. **??**, **??**) of the detail

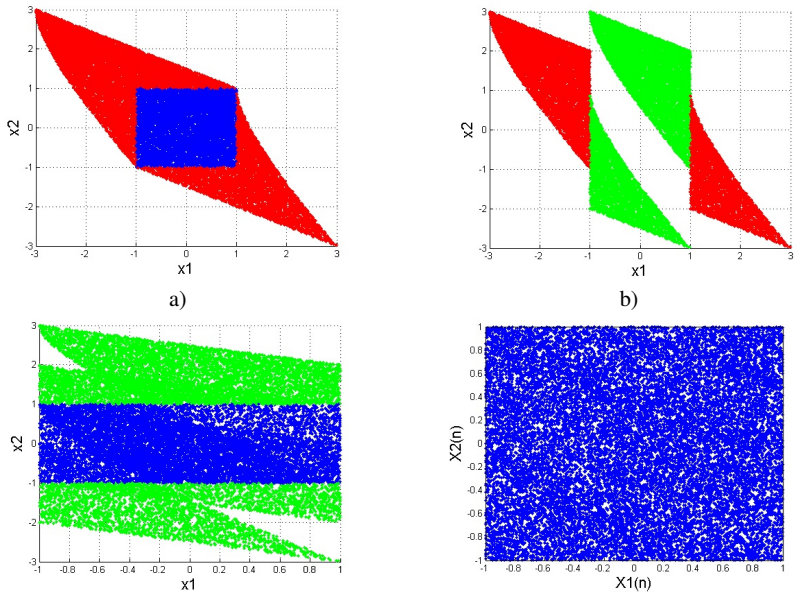


Fig. 1.8 Injection mechanism $[-3,3]^2 \Rightarrow [-1,1]^2$ for TTL_2^{SC} alternative map **a)** 2-D chaotic map without adding / substruction **b)** injection $x_n^{(1)}$ to the torus $[-1,1]^2$ **c)** injection $x_n^{(2)}$ to the torus $[-1,1]^2$ **d)** results after passing injection mechanism

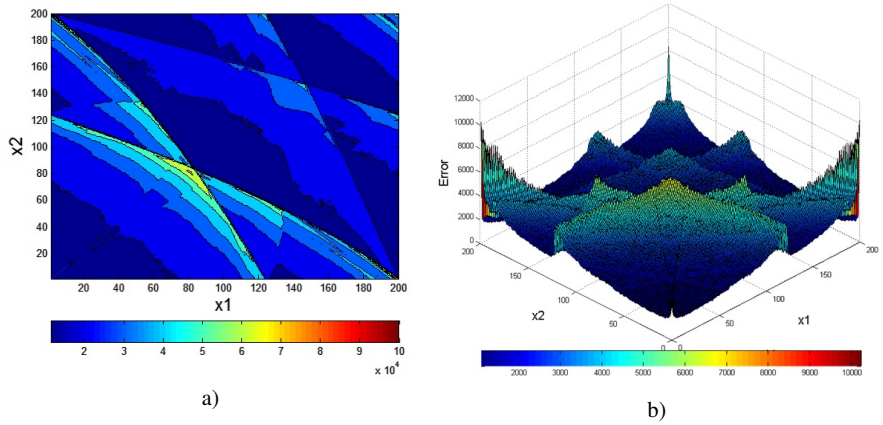
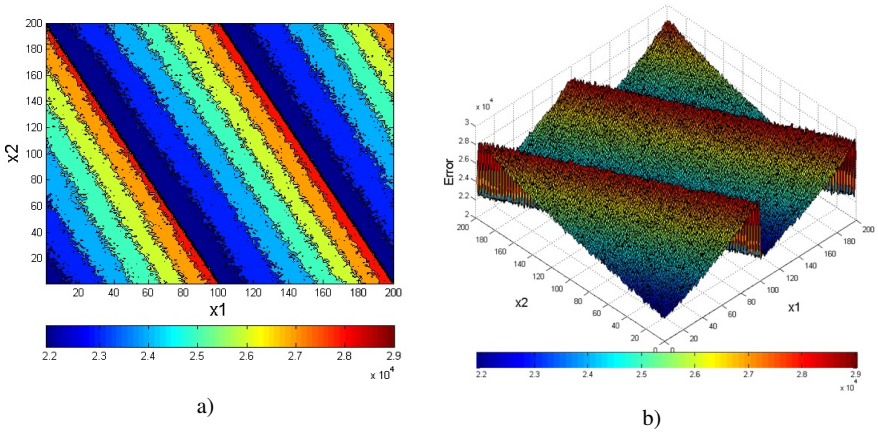


Fig. 1.9 Approximate density function of TTL_2^{RC} non-alternative map, where $step = 0.01$, 10^9 points are generated

points distribution demonstrates that both systems have not excellent distribution in phase space.



a) b)

Fig. 1.10 Approximate density function of TTL_2^{SC} alternative map, where $step = 0.01$, 10^9 points are generated

It was noticed that some parts of the graph (**??**.b) are perfectly joined, giving us idea to improve points density using some correction in equations.

1.3.3 A new 2-D chaotic PRNG

Considering the results of section 1.3.2. it seems possible to improve the randomness of the 2-D topology. We observe that two regions (top-green and right-red) on the Fig. **??**.b could be pretty connected. First, let us rewrite the mapping TTL_{μ}^{SC} alternative (**??**) where $\mu = 2$ as follow:

$$TTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 4|x_n^{(1)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(|x_n^{(1)}| - |x_n^{(2)}|) \end{cases} \tag{1.24}$$

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

$$MTTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 2|x_n^{(1)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(|x_n^{(1)}| - |x_n^{(2)}|) \end{cases} \tag{1.25}$$

and the injection mechanism (**??**) is used as well, but restricted to 3 phases:

$$\begin{array}{c} if\ x_{n+1}^{(1)} > 1\ then\ substract\ 2 \\ if\ x_{n+1}^{(2)} < -1\ then\ add\ 2 \\ if\ x_{n+1}^{(2)} > 1\ then\ substract\ 2 \end{array} \tag{1.26}$$

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

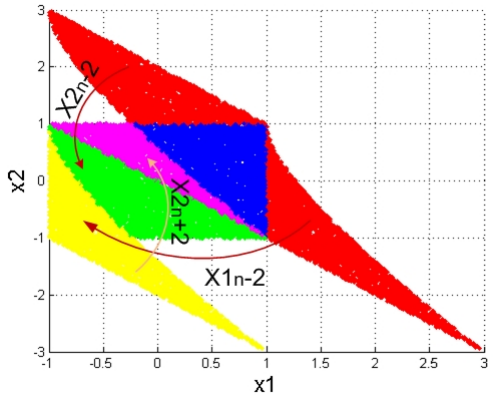


Fig. 1.11 Injection mechanism (**??**) of $MTTL_2^{SC}$ alternative map

The numerical results of the errors distributions (Fig. **??**) 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.

Table 1.1 Approximate distribution errors (**??**, **??**, **??**), for the system (**??**) in phase space

Points	$x^{(i)}x^{(j)}$	$ErrorL1$	$ErrorL2$	$ErrorL3$
10^4	$x^{(1)}x^{(2)}$	1.55830000000011	3.9967999999983	16
10^6	$x^{(1)}x^{(2)}$	0.158120000000055	0.395695199999969	1.56
10^8	$x^{(1)}x^{(2)}$	0.0159890999999995	0.0401757055999971	0.1748
10^9	$x^{(1)}x^{(2)}$	0.00505406199999996	0.00401402468000009	0.04916

The graph (Fig. **??**) shows straight error reducing that proves uniform points distribution.

The points distribution of the attractor in phase delay is quite good as well (Figs. **??**, **??**), where the plotting of 10^9 points are generated. On the Fig. (**??**b) tent distribution is recognized for $x^{(2)}$ variable but for encryption we need only output of one

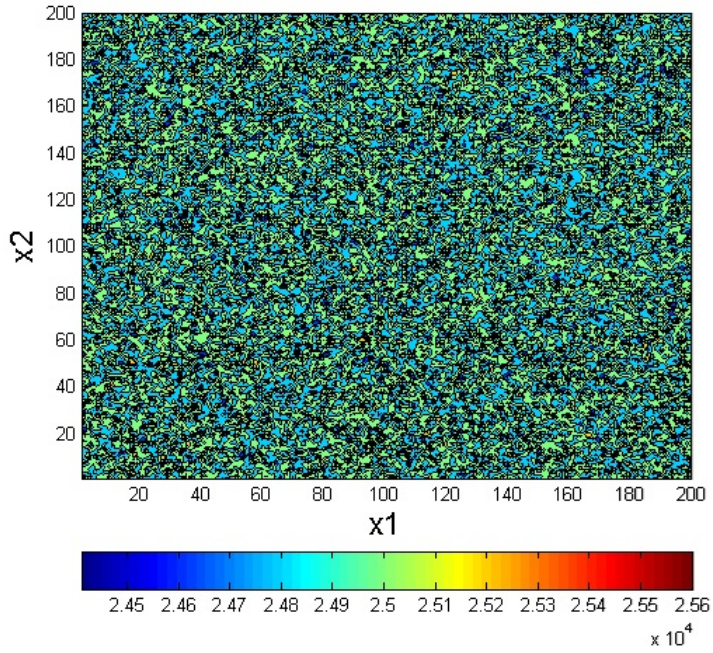


Fig. 1.12 Approximate density function of $MTTL_2^{SC}$ alternative map, where $step = 0.01$, 10^9 points are generated

state (in our case $x^{(1)}$). Both states make strong impact on itself and for the global dynamics reaching significant points distribution on the torus and chaoticity.

The $MTTL_2^{SC}$ alternative map is ring- and auto-coupled. Since one state takes part on creating dynamics of other one, both auto-correlation and cross-correlation have to be analysed for dependency and repeatability. The results of the 2-dimensional system are represented on the Fig. **??** and Fig. **??**. The same excellent results are on the Fig. **??** for autocorrelation, and on the Fig. **??** for cross-correlation, where the sequences on the graphs are near zero.

Topologically mixing means the system capability to progress over a short period of time. The system from any given initial region or open set of its phase space will ultimately mixed up with any other region so that it is impossible to predict system evolution.

Here we represent graphical analysis of the 2-D $MTTL_2^{SC}$ alternative map for topological mixing. The square $[0,1]^2$ is divided into 4 quadrants and each of them are split in boxes as well $(A2, B2, C2, \cdots, O2)$. 5×10^3 points have been generated in each of the boxes (Fig. **??**) and on the Fig.**??**.a-e it is showed where the points from the initial boxes $(A1, B1, C1, \cdots, O1)$ of quadrant are mapped.

From the Fig. **??** it can be seen that points are distributed everywhere over the square, and it is hard to predict the next point or to find the previous one. The system is perfectly mixing because the regions are superimposed to each other. For example

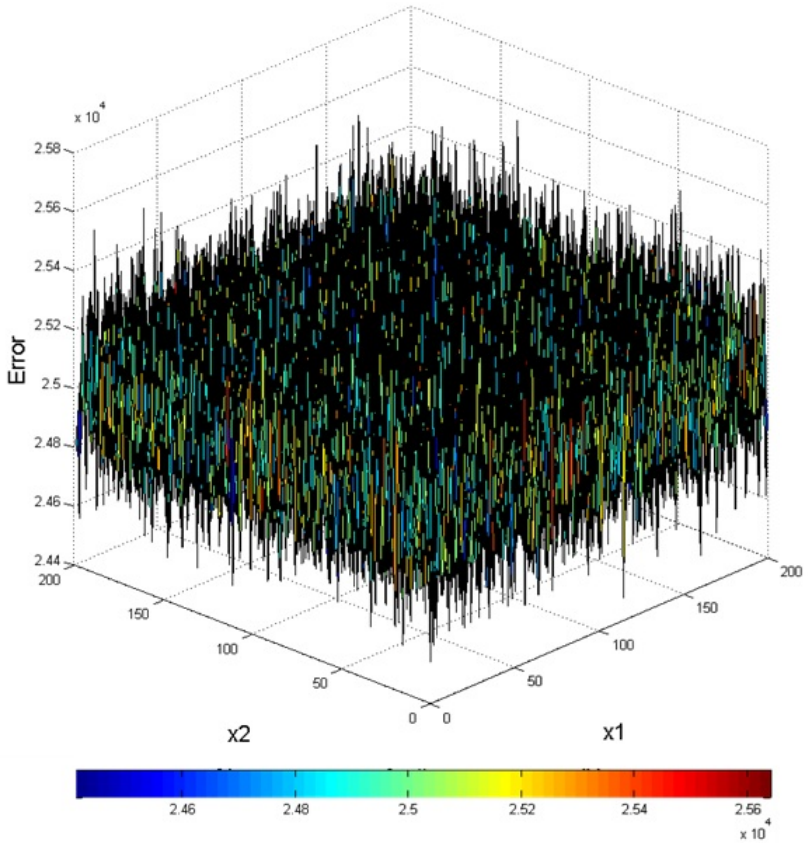


Fig. 1.13 Approximate density function in 3D of $MTTL_2^{SC}$ alternative map, where $step = 0.01$, 10^9 points are generated

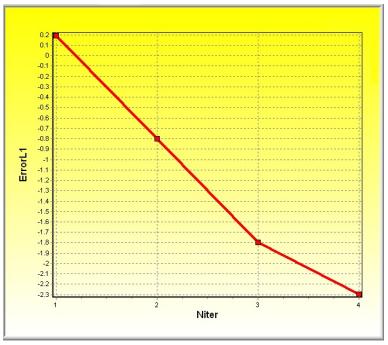


Fig. 1.14 Approximate distribution errors (**??**), for the system (**??**)

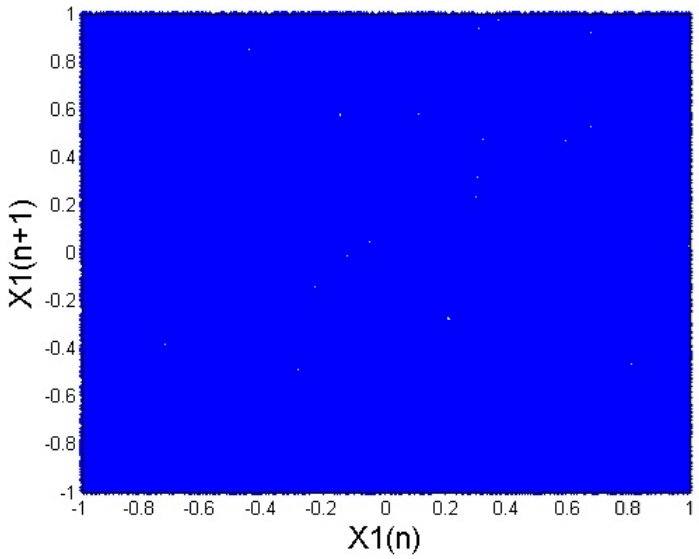


Fig. 1.15 Attractor in the phase delay $((x_n^{(1)}, x_{n+1}^{(1)}))$, 10^9 points are generated, for the system (**??**)

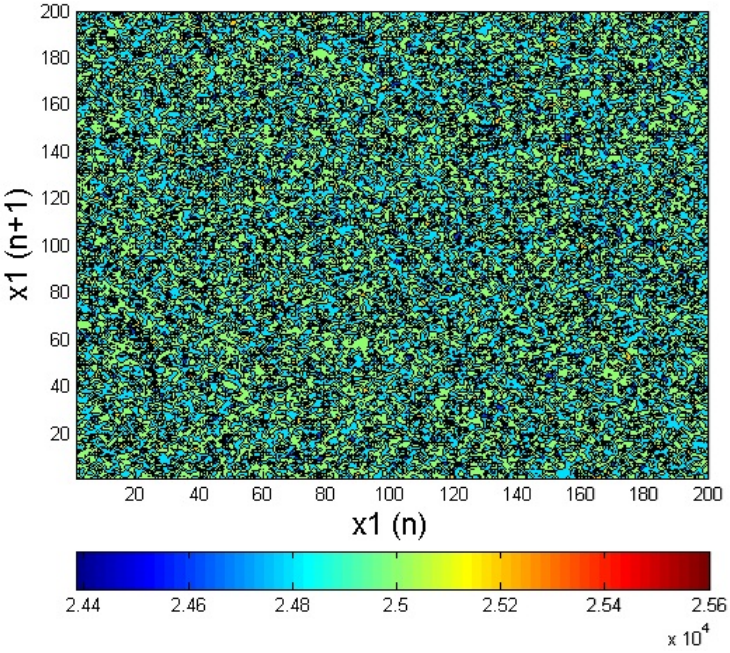


Fig. 1.16 Attractor in the phase delay $((x_n^{(1)}, x_{n+1}^{(1)}))$, box-method, 10^9 points are generated, for the system (**??**)

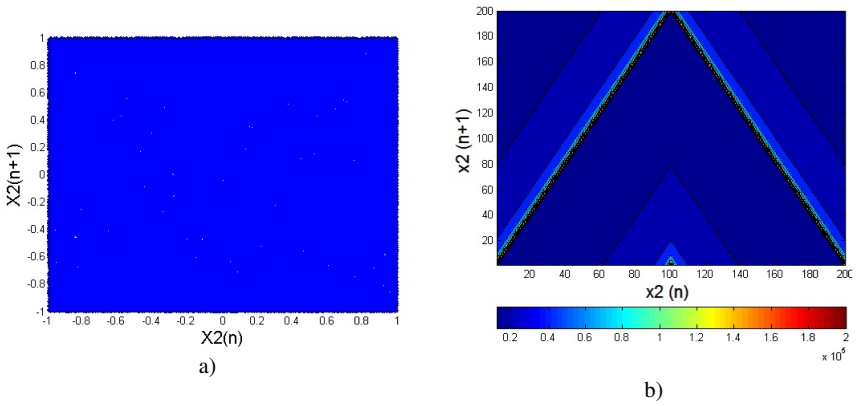


Fig. 1.17 Attractor in the phase delay, 10^9 points are generated a) $(x_n^{(2)}, x_{n+1}^{(2)})$ b) Box-method

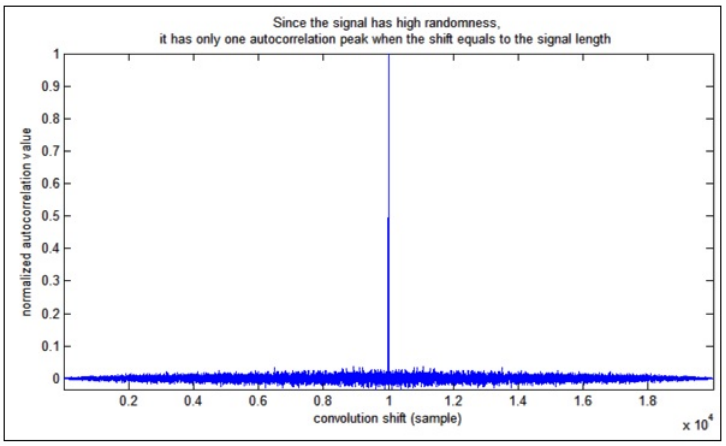


Fig. 1.18 State auto-correlation analysis of the $MTTL_2^{SC}$ alternative map

if we take some point of the $A2$ box (Fig. **??** the next point will fall down to the A2 region (Fig. **??**.a). The blue coloured region on the Fig. **??**.a passes through the boxes: $O1, I1, P1, C1, B1, E1, H1, M4, N4$ (Fig. **??**), that means the next points will fall down somewhere on the regions corresponding to these boxes (Fig.**??**.a-e). With all next iterations, they mix more complexely; the behavior becomes unpredictable and eventually looks like scattered points everywhere across the space. Colours and letters overlapping on the graphs vividly demonstrate that arbitrarily close points in some periods of time will have vastly different behaviors which means mixing. This phenomenon is quantified through the value of Largest lyapunov exponent. The arbitrarily taken points which are far alone will ultimately approach looking nearly the same only for several iterations means mixing as well. Since the new map implies of strong chaos, the phase space is thoroughly mixed together after a

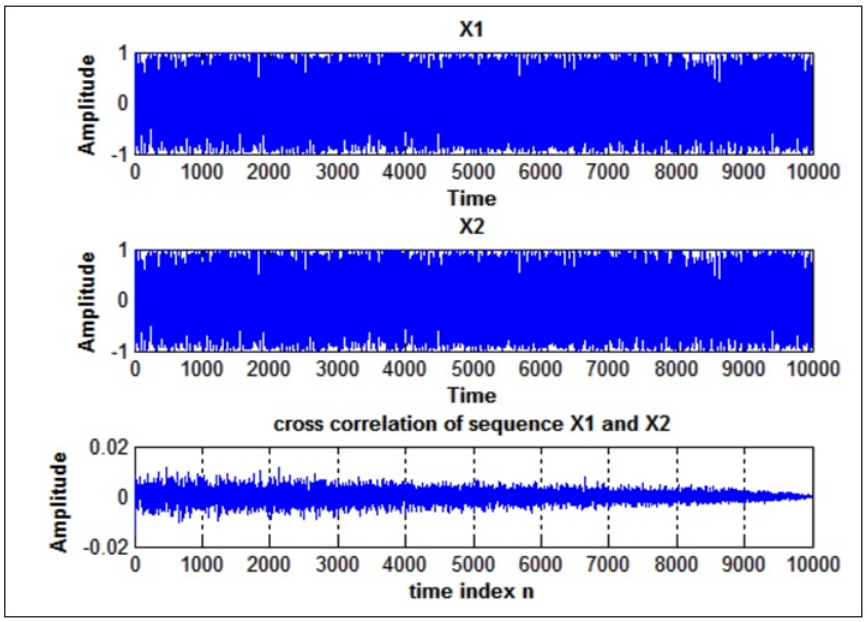


Fig. 1.19 Correlation between states of the $MTTL_2^{SC}$ alternative map

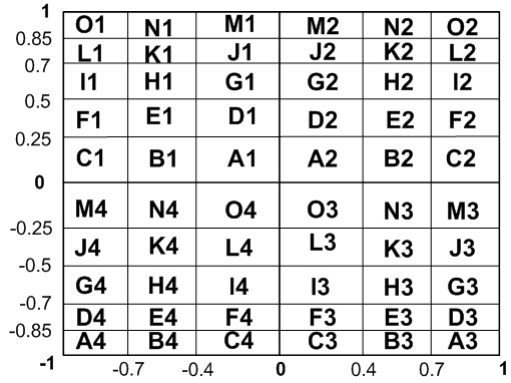


Fig. 1.20 Initial boxes $(A,B,C,\cdots,O)$ in the four quadrants

quite short time. In a forthcoming paper we will quantify this mixing, building a corresponding Markov transition matrix as in [**?**].

NIST tests are used to verify randomness and system capability to resist main attacks. As it was earlier discussed the advantage of the binary sequences has to be approximately the same as of the truly random number generator. NIST tests are more fully cover the statistical tests. Long time the tests are used to prove PRNG robustness. NIST tests require only binary sequences, thus 4×10^6 points were gen-

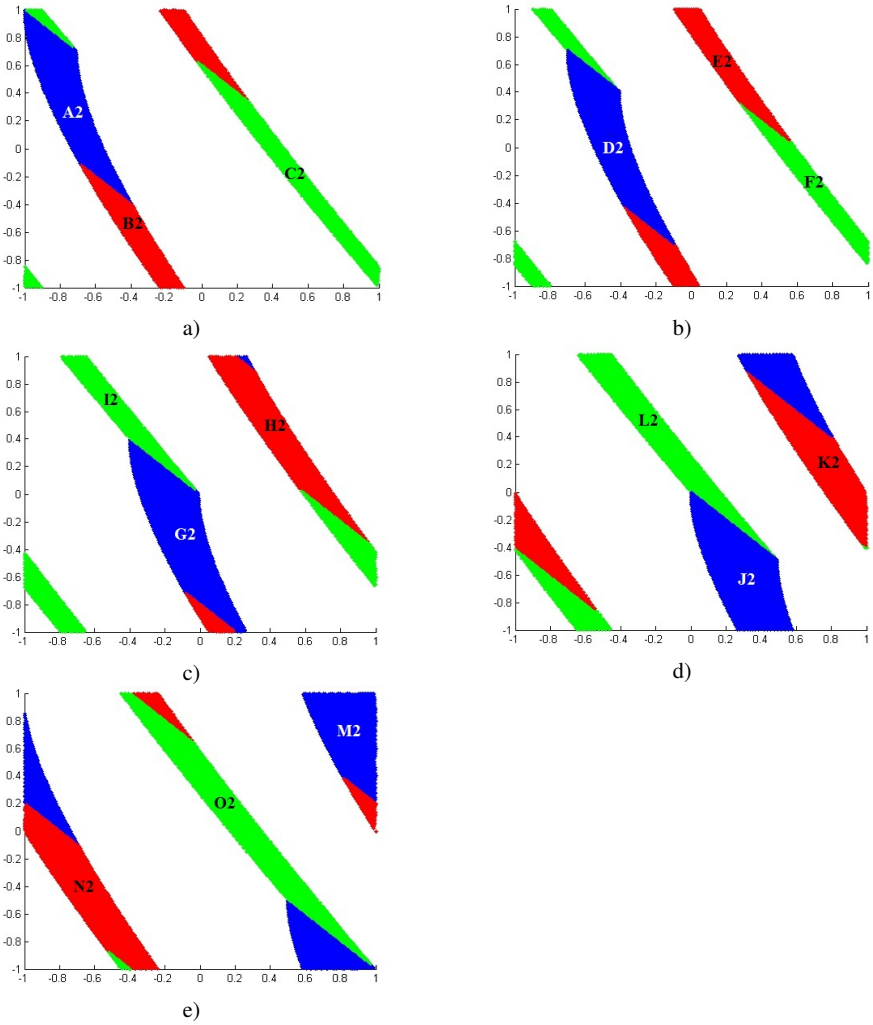


Fig. 1.21 Topological mixing

erated, the first 5×10^5 were cut off. The rest of the sequence was converted to binary form according to the standard IEEE-754 (32 bit single precision floats).

Both states of the generator successfully passed NIST tests demonstrating strong randomness being robustness against numerous statistical attacks (Fig. **??**). Moreover, we can say that generated sequences look like truly random. Thus, if the adversary looks at the sequence it will be difficult to distinguish it from a truly random generator.

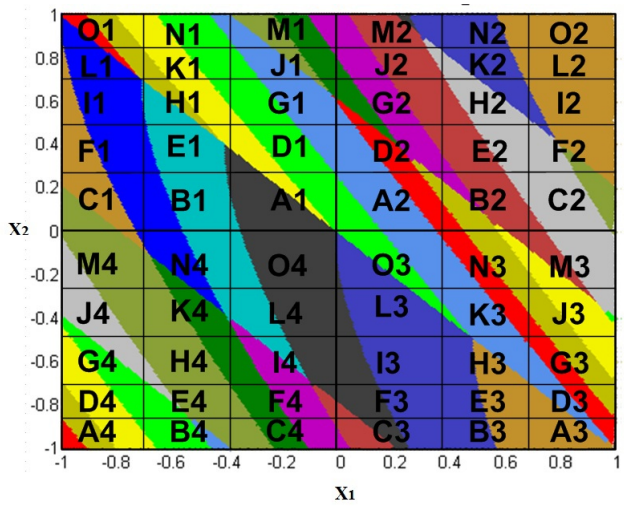


Fig. 1.22 Mixing boxes ($A \dots O$) and regions (coloured) in the phase space $(x_n^{(1)}, x_n^{(2)})$

1.4 A new higher-dimensional map

Higher dimensional systems allow to achieve the best randomness, chaoticity and points distribution, because there are more perturbations and nonlinear mixing in it. Usually, 3 or more dimensions are enough to create robust random sequences. Thus, it is an advantage if the system could increase its dimensions. Since, $MTTL_2^{SC}$ alternative map cannot be in higher dimension, we describe how to improve randomness, best points distribution and more complex dynamics than $TTL_2^{RC}(x^{(2)}, x^{(1)})$ alternative map (**??**).

The best way to achieve randomness from chaos is to couple states with auto and ring-coupling [**?**]. After applying the conditions the higher dimension map takes form as follow:

$$TTL_2^{RC}: \begin{cases} x_{n+1}^{(1)} = 1 - 2|x_n^{(1)}| + 2(|x_n^{(2)}| - (x_n^{(1)})^2) \\ x_{n+1}^{(2)} = 1 - 2|x_n^{(2)}| + 2(|x_n^{(3)}| - (x_n^{(2)})^2) \\ \vdots \\ x_{n+1}^{(p)} = 1 - 2|x_n^{(p)}| + 2(|x_n^{(1)}| - (x_n^{(p)})^2) \end{cases} \tag{1.27}$$

The injection is applied as well by verifying each of the state for diverging, in the case if, the injection is used.

Note, each of the states has to satisfy requirements and chaoticity. Therefore, the 3-D and 4-D system were studied for criteria 1-8 (Fig. **??**) independently for the each states and in correlation between them. All of the tests have been successfully passed with improving results whereas dimension is higher. Here we demonstrate only more significant and important tests.

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

generator is <data/Modified TL_{\mu}^{SC} alternative map_x1.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	8	11	9	10	8	11	15	11	9	0.897763	100/100	Frequency
13	13	12	7	11	10	12	9	5	8	0.678686	99/100	BlockFrequency
6	7	5	12	16	12	12	9	14	7	0.191687	100/100	CumulativeSums
8	10	12	6	14	12	9	6	12	11	0.678686	100/100	Runs
14	11	12	10	15	5	6	13	8	6	0.236810	99/100	LongestRun
9	6	13	10	7	10	11	11	12	11	0.897763	97/100	Rank
11	12	6	19	4	11	11	13	8	5	0.037566	97/100	FFT
7	9	13	14	12	9	9	11	7	9	0.816537	100/100	NonOverlappingTemplate
10	11	15	10	11	9	12	6	11	5	0.595549	98/100	OverlappingTemplate
11	10	5	7	5	13	16	5	13	15	0.058984	100/100	Universal
14	6	11	10	7	9	13	12	8	10	0.739918	98/100	ApproximateEntropy
2	9	7	8	5	7	5	5	8	7	0.689019	63/63	RandomExcursions
5	8	4	4	6	4	4	11	6	11	0.222869	63/63	RandomExcursionsVariant
12	10	12	13	7	8	7	7	6	18	0.171867	99/100	Serial
9	13	11	12	7	9	7	16	7	9	0.534146	99/100	LinearComplexity

a)

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

generator is <data/Modified TL_{\mu}^{SC} alternative map_x2.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
18	6	8	12	9	6	7	10	11	13	0.191687	98/100	Frequency
12	7	12	7	3	11	13	10	13	12	0.366918	98/100	BlockFrequency
15	14	8	6	8	13	7	10	9	10	0.494392	98/100	CumulativeSums
12	15	11	8	7	12	9	5	8	13	0.474986	98/100	Runs
9	12	13	13	9	14	9	6	8	7	0.637119	100/100	LongestRun
8	12	8	10	13	15	10	6	7	11	0.616305	98/100	Rank
8	12	9	15	9	8	17	9	9	4	0.181557	99/100	FFT
7	12	7	12	6	9	15	12	7	13	0.437274	100/100	NonOverlappingTemplate
9	12	11	3	16	8	10	13	10	8	0.289667	99/100	OverlappingTemplate
9	13	10	6	8	8	11	10	11	14	0.816537	99/100	Universal
7	24	9	7	7	8	8	17	7	6	0.000347	98/100	ApproximateEntropy
2	4	2	5	5	7	2	13	4	8	0.011791	52/52	RandomExcursions
5	4	8	5	2	1	8	6	4	9	0.191687	52/52	RandomExcursionsVariant
6	10	8	7	15	15	15	8	8	8	0.236810	100/100	Serial
7	9	11	11	6	15	7	11	8	15	0.419021	99/100	LinearComplexity

b)

Fig. 1.23 $MTTL_2^{SC}$ alternative map successfully passed NIST tests a) $x^{(1)}$ b) $x^{(2)}$

First of all, the points distribution is the best tool to demonstrate the system evolution with increasing dimension. Therefore, to draw the plot 10^9 points were generated for: 2-D, 3-D and 4-D system. The invariant measure was calculated with distribution error results fixing on the iterations: 10^4, 10^6, 10^8 and 10^9. The graph (Fig. **??**) shows improving the points distribution the space.

After generating 10^6 points for 2-D system sequences become repeatable because the errors no longer decrease. This phenomenon may be due to long periodic orbits attracting the behaviour of iterated points. For 3-D system period is longer but is locked after 10^9 generated points because errors should be reduced 10 times on each $100 \times length$. Note, when length goes to infinity ($length = 10^{11}$, for example) the error no longer decreases. The systems distribution errors comparison is demonstrated on Fig. **??**.

The robust PRNG implies the points to have equal chance to be chosen. Thus, the system appears to be unpredictable. The precise comparison can be made by

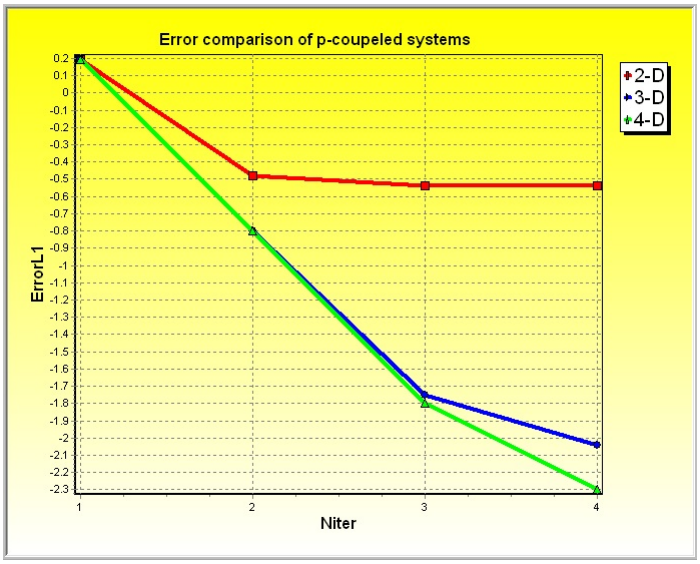


Fig. 1.24 Density error (**??**) for: 2-D, 3-D and 4-D $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map

numerical calculation to compare deviation from etalon distribution: ErrorL1 (**??**), ErrorL2 (**??**) and ErrorL3 (**??**). The table (**??**) displays numerical results for 3-D map and in (Tab. **??**) for 4-D $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map are demonstrated.

Table 1.2 Numerical results of the error points distribution for 3-D $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map

Points	$x^{(i)}x^{(j)}$	$ErrorL1$	$ErrorL2$	$ErrorL3$
10^4	$x^{(1)}x^{(2)}$	1.55695000000012	3.98719999999827	16
10^4	$x^{(1)}x^{(3)}$	1.55960000000011	4.02879999999834	16
10^4	$x^{(2)}x^{(3)}$	1.55850000000012	4.0111999999983	16
10^6	$x^{(1)}x^{(2)}$	0.160244000000057	0.406133599999969	1.56
10^6	$x^{(1)}x^{(3)}$	0.159324000000056	0.400406399999964	1.72
10^6	$x^{(2)}x^{(3)}$	0.159722000000056	0.401812799999966	1.64
10^8	$x^{(1)}x^{(2)}$	0.0175167799999997	0.0483318551999966	0.1788
10^8	$x^{(1)}x^{(3)}$	0.0176578999999997	0.0488421623999967	0.1784
10^8	$x^{(2)}x^{(3)}$	0.0176171399999997	0.0485752623999967	0.1836
10^9	$x^{(1)}x^{(2)}$	0.00908920799999996	0.0125199035839995	0.0772
10^9	$x^{(1)}x^{(3)}$	0.00903516200000002	0.0124306507039994	0.08368
10^9	$x^{(2)}x^{(3)}$	0.00907240999999998	0.0124629701279995	0.07804

The numerical results demonstrate harmony of the points density between states. Moreover, the NIST tests prove it randomness (Fig. **??**).

Table 1.3 Numerical results of the error points distribution for 4-D $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map

Points	$x^{(i)}x^{(j)}$	$ErrorL1$	$ErrorL2$	$ErrorL3$
10^4	$x^{(1)}x^{(2)}$	1.55720000000011	3.9991999999983	16
10^4	$x^{(1)}x^{(3)}$	1.55655000000012	3.96879999999831	16
10^4	$x^{(1)}x^{(4)}$	1.55495000000012	3.95519999999832	20
10^4	$x^{(2)}x^{(3)}$	1.5581000000001	4.0063999999983	16
10^4	$x^{(2)}x^{(4)}$	1.5576000000001	4.0047999999983	16
10^4	$x^{(3)}x^{(4)}$	1.55395000000012	3.93519999999834	16
10^6	$x^{(1)}x^{(2)}$	0.158570000000055	0.398432799999969	1.64
10^6	$x^{(1)}x^{(3)}$	0.159702000000056	0.404377599999966	1.68
10^6	$x^{(1)}x^{(4)}$	0.160002000000056	0.405107199999971	1.64
10^6	$x^{(2)}x^{(3)}$	0.158936000000056	0.399593599999971	1.52
10^6	$x^{(2)}x^{(4)}$	0.159348000000055	0.401847999999965	1.68
10^6	$x^{(3)}x^{(4)}$	0.158972000000057	0.399148799999965	1.72
10^8	$x^{(1)}x^{(2)}$	0.0159831399999994	0.0400194487999969	0.1608
10^8	$x^{(1)}x^{(3)}$	0.0160255399999995	0.040381923199997	0.1772
10^8	$x^{(1)}x^{(4)}$	0.0160366599999995	0.0404230903999969	0.1852
10^8	$x^{(2)}x^{(3)}$	0.0160441999999995	0.0403678407999969	0.1732
10^8	$x^{(2)}x^{(4)}$	0.0158792799999996	0.0396031839999973	0.1612
10^8	$x^{(3)}x^{(4)}$	0.0158101199999993	0.039183199999997	0.164
10^9	$x^{(1)}x^{(2)}$	0.00507232799999997	0.00404898352000012	0.0524
10^9	$x^{(1)}x^{(3)}$	0.00515058999999998	0.00415637283200005	0.05388
10^9	$x^{(1)}x^{(4)}$	0.00504731199999992	0.00399370235200004	0.05932
10^9	$x^{(2)}x^{(3)}$	0.00505795999999996	0.00400627627200004	0.05516
10^9	$x^{(2)}x^{(4)}$	0.00514836599999991	0.00416637750400014	0.05228
10^9	$x^{(3)}x^{(4)}$	0.00503734799999993	0.00397888753600011	0.05112

1.5 Conclusion

In this paper we have proposed the original idea to couple two well-known chaotic maps (tent and logistic one), which considered separately - don't exhibit the required features for encryption purposes. However, the new coupling changed qualitatively the overall system behavior, because the maps used with injection mechanism and coupling between states increas their complexity.

We have explored several topologies and finally proposed a new 2-D CPRNG. The proposed model with injection mechanism allows 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 $MTTL_2^{SC}$ alternative 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 great 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,

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	14	8	9	10	9	11	12	6	13	0.779188	100/100	Frequency
11	9	9	8	6	15	7	13	9	13	0.574903	100/100	BlockFrequency
14	6	13	7	11	5	10	11	9	14	0.401199	100/100	CumulativeSums
12	10	7	7	16	8	13	7	13	7	0.366918	99/100	CumulativeSums
16	9	7	11	14	12	6	13	7	5	0.181557	100/100	Runs
13	9	14	11	11	8	9	12	5	8	0.678686	100/100	LongestRun
14	9	7	8	9	16	9	12	6	10	0.455937	100/100	Rank
13	4	9	11	7	4	10	12	19	11	0.037566	100/100	FFT
14	8	8	9	8	15	11	11	8	8	0.699313	100/100	NonOverlappingTemplate
14	15	12	10	6	9	13	7	3	11	0.162606	99/100	OverlappingTemplate
8	7	11	16	9	12	10	9	7	11	0.678686	100/100	Universal
13	11	10	12	6	12	12	14	6	4	0.304126	97/100	ApproximateEntropy
5	5	6	9	2	7	5	8	9	6	0.637119	62/62	RandomExcursions
6	2	4	9	6	11	6	5	6	7	0.407091	62/62	RandomExcursionsVariant
13	8	15	8	12	9	7	15	8	5	0.275709	99/100	Serial
13	6	15	12	11	6	15	8	8	6	0.213309	99/100	Serial
9	6	8	13	8	11	10	11	12	12	0.883171	99/100	LinearComplexity

b)

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	5	12	14	10	9	12	16	8	7	0.289667	99/100	Frequency
7	7	9	10	6	10	14	8	10	19	0.137282	99/100	BlockFrequency
8	2	9	16	13	9	13	9	7	14	0.090936	99/100	CumulativeSums
5	8	14	11	11	11	14	5	10	11	0.437274	99/100	CumulativeSums
6	16	13	11	9	10	8	7	11	9	0.554420	100/100	Runs
9	13	6	9	14	10	8	11	12	8	0.779188	99/100	LongestRun
9	8	14	6	12	12	8	10	8	13	0.719747	100/100	Rank
10	10	17	5	9	13	14	10	6	6	0.153763	99/100	FFT
9	7	9	13	9	10	10	14	6	13	0.719747	100/100	NonOverlappingTemplate
5	9	12	7	7	12	12	13	12	11	0.637119	99/100	OverlappingTemplate
12	16	8	7	9	10	7	12	8	11	0.616305	99/100	Universal
8	16	6	12	11	13	5	7	13	9	0.249284	99/100	ApproximateEntropy
4	8	4	6	8	5	7	8	9	7	0.804337	66/66	RandomExcursions
4	7	7	8	2	8	6	8	7	9	0.602458	66/66	RandomExcursionsVariant
11	10	10	18	6	5	11	12	10	7	0.213309	100/100	Serial
8	11	10	10	12	11	10	9	9	10	0.998821	98/100	Serial
10	7	13	11	8	7	11	14	11	8	0.798139	99/100	LinearComplexity

c)

Fig. 1.25 NIST tests for **b)** 3-D $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map **b)** 4-D $TTL_2^{RC}(x^{(2)},x^{(1)})$ alternative map

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 dynamics making the system strong-potential candidate for high-security applications. Finally, the dimension of the TTL_μ^{RC} non-alternative map is easily increased whenever it is necessary to reach the strongest security requirements as shown in Sec.1.4.

References

1. Abraham, J., P. Abreu, M. Aglietta, C. Aguirre, D. Allard, I. Allekotte: Correlation of the highest-energy cosmic rays with nearby extragalactic objects. Science **5852**, 938-943. (2007)
2. Alvarez, G., S. Li: Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos **16**, 2129-2151 (2006)
3. Ariffin, M. R. K., M. S. M. Noorani: Modified Baptista type chaotic cryptosystem via matrix secret key. Physics Letters A **372**, 5427-5430 (2008)
4. Banerjee, S., D. Kastha, S. Das, G. Vivek, C. Grebogi: Robust chaos-the theoretical formulation and experimental evidence. IEEE International Conference on. **5**, 293-296 (1999)

5. Banks, J., J. Brooks, G. Cairns, G. Davis, P. Stacey: On Devaney's definition of chaos. American Mathematical Monthly, 332-334 (1992)
6. Baptista, M. S: Cryptography with chaos. Physics Letters A. **240**, 50-54 (1998)
7. Boneh, D., B. Waters: Constrained pseudorandom functions and their applications. In Advances in Cryptology-Asiacrypt, 280-300. (2013)
8. Dachselt, F., W.S. Schwarz: Chaos and cryptography. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on **48**, 1498-1509 (2001)
9. Dogan, R., A. T. Murgan, S. Ortmann, M. Glesner: Searching for robust chaos in discrete time neural networks using weight space exploration. IEEE International Conference on. **2**, 688-693 (1996)
10. Dowell, E. H., C. Pezeshki: On the understanding of chaos in Duffings equation including a comparison with experiment. Journal of Applied Mechanics. **55**, 5-9 (1986)
11. Feki, M.: An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons and Fractals. **18 (1)**, 141-148 (2003)
12. Feigenbaum, M. J: The universal metric properties of nonlinear transformations. Journal of Statistical Physics. **21 (6)**, 669-706 (1979)
13. Frey, D. R, W. Schwarz: Chaotic digital encoding: an approach to secure communication. Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on **40**, 660-666 (1993)
14. Garasym, O., I. Taralova, R. Lozi: Application of nonlinear dynamics to chaotic prng design. European conferance on iteration theory (ECIT), 2014 International Conference on, 20. (2014)
15. Li, C., G. Chen: Chaos in the fractional order Chen system and its control. Chaos, Solitons and Fractals. **22**, 549-554 (2004)
16. Heidari-Bateni, G., C. D. McGillem: A chaotic direct-sequence spread-spectrum communication system. Communications, IEEE Transactions on **42**, 1524-1527. (1994)
17. Holenstein, T: Pseudorandom generators from one-way functions: A simple construction for any hardness. In Theory of Cryptography, 443-461. (2006)
18. Hong, Z., X. Ling: Generating chaotic secure sequences with desired statistical properties and high security. International Journal of Bifurcation and Chaos **7**, 205-213 (1997)
19. Jarecki, S., X. Liu: Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection. In Theory of Cryptography, 577-594. (2009)
20. XiongJ., Z. Yang: Chaos caused by a topologically mixing map. International Centre for Theoretical Physics. (1991)
21. Katz, O., D. A. Ramon, I. A. Wagner: A robust random number generator based on a differential current-mode chaos. IEEE Transactions on . **16**, 1677-1686 (2008)
22. Lanford III, O. E: Informal remarks on the orbit structure of discrete approximations to chaotic maps. Experimental Mathematics **7**, 317-324. (1998)
23. Li, C.-Y., Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, T. Kiwing: Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on **20 (2)**, 385-389. (2012)
24. Liebert, W., H. G. Schuster: Proper choice of the time delay for the analysis of chaotic time series. Physics Letters A. **142**, 107-111 (1989)
25. Lozi, R: Chaotic pseudo random number generators via ultra weak coupling of chaotic maps and double threshold sampling sequences, In ICCSA 2009, 3rd Conference on Complex Systems and Applications, 20-24. (2009)
26. Lozi, R., E. Cherrier: Noise-resisting ciphering based on a chaotic multi-stream pseudo-random number generator, in. n Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, 91-96. (2011)
27. Lozi, R: Emergence of randomness from chaos. International Journal of Bifurcation and Chaos **22(02)**, 1250021?1/15. (2012)
28. Lozi, R: Can we trust in numerical computations of chaotic solutions of dynamical systems?. In Topology and dynamics of Chaos, World Scientific Series in Nonlinea Science Series A. **84**, 63-98. (2013)

29. Lozi, R., I. Taralova: From chaos to randomness via geometric undersampling. ESAIM: Proceedings and surveys, November 14. **46**, 177-195. (2014)
30. Ma, H.-G., C.-Z. Han: Selection of embedding dimension and delay time in phase space reconstruction. Frontiers of Electrical and Electronic Engineering in China 1. **1**, 111-114. (2006)
31. May, R: Stability and Complexity of Models Ecosystems. Princeton University Press, Princeton NJ. (1973)
32. May, R: Biological populations with overlapping generations: stable points, stable cycles, and chaos. Science **186 (4164)**, 645-647. (1974)
33. Menezes, A. J., P. C. Van Oorschot: Handbook of applied cryptography. CRC press. (1996)
34. Nejati, H., A. Beirami, Y. Massoud: A realizable modified tent map for true random number generation. In Circuits and Systems, 2008. MWSCAS **10**, 621-624. (2008)
35. Nillsen, R: Randomness and recurrence in dynamical systems. AMC **10**, 12-30. (2010)
36. Noura, H., S. El Assad, C. Vladeanu: Design of a fast and robust chaos-based cryptosystem for image encryption. In Communications (COMM), 2010 8th International Conference on, 423-426. (2010)
37. Odibat, Z. M., N. Corson, M. A. Aziz-Alaoui, C. Bertelle: Synchronization of chaotic fractional-order systems via linear control. International Journal of Bifurcation and Chaos **20**, 81-97. (2010)
38. Pichler, L., H. J. Pradlwarter: Evolution of probability densities in the phase space for reliability analysis of non-linear structures. Structural Safety **31**, 316-324. (2009)
39. Reingold, O: Theory of Cryptography. In 6th theory of cryptography conference, tcc, 15-17. (2009)
40. Rojas, A., I. Taralova, R. Lozi: New alternate ring-coupled map for multirandom number generation. Journal of Nonlinear Systems and Applications **4(1)**, 64-69. (2013)
41. Rukhin, A., J. Soto, J. Nechvatal, M. Smid, E. Barker: A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-allen and hamilton inc mclean va. (2010)
42. Sato, S., M. Sano, Y. Sawada: Practical methods of measuring the generalized dimension and the largest Lyapunov exponent in high dimensional chaotic systems. Progress of Theoretical Physics. **77**, 1-5 (1987)
43. Shengqiang, L., C. Zhixiong, S. Rong, X. I. Guozhen: In the randomness of generalized cyclotomic sequences of order two. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **90**, 2037-2041. (2007)
44. Singh, A., R. Gilhotra: Data security using private key encryption system based on arithmetic coding. International Journal of Network Security and Its Applications (IJNSA) **3**, 58-67. (2011)
45. Sprott, J. C.: Chaos and time-series analysis. Oxford: Oxford University Press **69**. (2003)
46. Sudret, B.: Global sensitivity analysis using polynomial chaos expansions. Reliability Engineering and System Safety **93**, 964-979 (2008)
47. Sundarapandian, V., I. Pehlivan: Analysis, control, synchronization, and circuit design of a novel chaotic system. Mathematical and Computer Modelling **12**, 1904-1915. (2012)
48. Thiffeault, J.-L., M. D. Finn, E. Gouillart, T. Hall: Topology of chaotic mixing patterns. Chaos: An Interdisciplinary Journal of Nonlinear Science **18** (2008)
49. Wang, S., J. Kuang, J. Li, Y. Luo, H. Lu, G. Hu: Chaos-based secure communications in a large community. Physical Review E **66**, 065202. (2002)
50. Wong, W. K., L. P. Lee, K. W. Wong: A modified chaotic cryptographic method. In Communications and Multimedia Security Issues of the New Century, 123-126. (2001)
51. Yuan, G., J. A Yorke: Collapsing of chaos in one dimensional maps. Physica D: Nonlinear Phenomena **136**, 18-30. (2000)
52. Zaher, A. A., A.-R. Abdulnasser: On the design of chaos-based secure communication systems. Communications in Nonlinear Science and Numerical Simulation. **16 (9)**, 3721-3737 (2011)

53. Zhou, X., X. Tang: Research and implementation of RSA algorithm for encryption and decryption. In Strategic Technology (IFOST), 2011 6th International Forum on. **1**, 1118-1121 (2011)

Oleg Garasym and Ina Taralova
IRCCyN, UMR CNRS 6597 Ecole Centrale de Nantes, NANTES
France
oleg.garasym@irccyn.ec-nantes.fr
Ina.Taralova@irccyn.ec-nantes.fr

René Lozi
Laboratoire J. A. Dieudonné, UMR CNRS 7351 Nice Sophia-Antipolis, NICE
France
rlozi@unice.fr