Digitized Chaos for Pseudo-Random Number Generation in Cryptography

Tommaso Addabbo, Ada Fort, Santina Rocchi, Valerio Vignoli

Department of Information Engineering
University of Siena, 53100 Italy
(e-mail: addabbo@dii.unisi.it)

⋆ RESEARCH MANUSCRIPT ⋆

– PLEASE REFER TO THE PUBLISHED PAPER[1] –

1 Introduction

Random numbers play a key-role in cryptography, since they are used, e.g., to define enciphering keys or passwords [1]. Nowadays, the generation of random numbers is obtained referring to two types of devices, that are often properly combined together: True Random Number Generators (TRNGs), and Pseudo Random Number Generators (PRNGs). The former are devices that exploit truly stochastic physical phenomena [2–6], such as the electronic noise or the chaotic dynamics of certain nonlinear systems: for these devices the output sequences have an intrinsic degree of unpredictability, that is measured referring to the theoretical tools provided by Information Theory (e.g., in terms of the Shannon entropy) [4, 7]. On the other hand, PRNGs are deterministic periodic finite state machines whose aim is to emulate, within the period, the random behavior of a truly random source of numbers. From a theoretical point of view, due to their deterministic nature, PRNGs are potentially predictable by observing their generated sequences [1, 8–10]. Nevertheless, in literature some families of PRNGs are classified to be 'secure', meaning that their algorithmic structure involves calculations that *in average*, referring to the prediction task, require an amount of computation time that is *asymptotically* unfeasible with the size of the problem, when referring to both the computational equipment at disposal and the known computing fastest algorithms [1, 11]. It is worth noting that a given generator, even if belonging to an asymptotically secure family of PRNGs, can generate short periodic (and unsecure) sequences for several values of the initial seed[2]. Therefore, apart from the cryptographic robustness of their algorithmic structure, a cryptographic PRNG must generate sequences that are

[1] Chaos-Based Cryptography: Theory, Algorithms and Applications, 2011, L. Kocarev, and S. Lian (Ed.), vol. 354, Springer, p. 67-97

[2] E.g., the well known Blum, Blum, Shub generator $k_{n+1} = k_n^2 \bmod N$ can generate short periodic sequences (short compared to N).

acceptable from a statistical point of view, i.e., that pass a certain number of standard statistical tests [1, 12].

In this work we propose to take certain chaotic systems as a reference for the design of PRNGs based on nonlinear congruences. In detail, in Section 2 we report a brief comparison between linear and nonlinear PRNGs. Since our aim is to derive nonlinear congruential generators from certain chaotic maps, in Section 3 we overview some theoretical fundamentals about TRNGs based on statistically stable mixing dynamical systems, focusing on the family of the Rényi maps. In Section 4 we discuss the link that exists between the dynamics of chaotic and pseudo-chaotic systems: to explain how the two dynamics are related it is necessary to project some results achieved within the Ergodic Theory (valid for chaotic systems) on the world of digital pseudo-chaos. To this aim, we have proposed a weaker and more general interpretation of the Shadowing Theory proposed by Coomes et al. [13], focusing on probability measures, rather than on single chaotic trajectories. In Section 5 we study how to digitize the Rényi maps, discussing how to set a minimum period length of the digitized trajectories. In Section 6 we present two alternative methods for the design of PRNGs based on nonlinear recurrences derived from the Renyi map, reporting the results of the NIST SP800.22 standard statistical test suite [12].

2 Linear vs. nonlinear congruential generators

Conventional cryptographic systems are based on finite state machines, and the problem of generating random numbers can be analyzed referring to finite subsets of integers. Accordingly, let $\Lambda_M = \{0, \ldots, M\}$ be the set of the first $(M + 1)$ non-negative integers. We define the j-plet $k_0, \ldots, k_{j-1} \in \Lambda_M$ as the *initial seed* of the generator, and we define a congruential generator as an iterative method for generating the sequence $\{k_i \in \Lambda_M, i \in \mathbb{N}\}$, where

$$k_n = G(k_{n-1}, \ldots, k_{n-j}) \bmod M, \qquad n > j, \tag{1}$$

for a certain function $G : \Lambda_M^j \to \mathbb{N}$. The congruential generator is called linear if the function G is a linear combination of the previous j numbers in the sequence (with coefficients in Λ_M), otherwise it is said nonlinear. The simplest example of a linear generator of the form (1) is the Linear Congruential Generator (LCG) $k_n = ak_{n-1} + c \bmod M$, whereas for the Linear Feedback Shift Register (LFSR) with primitive polynomial $x^3 + x + 1$ we have $M = 2$, $\Lambda_2 = \{0, 1\}$ and $G(k_{n-1}, k_{n-2}, k_{n-3}) = k_{n-1} + k_{n-3}$ [10]. Examples of nonlinear congruential generators are the Nonlinear Feedback Shift Registers (NLFSRs), the polynomial congruential generators in which $G(k_{n-1}) = a_p k_{n-1}^p + a_{p-1} k_{n-1}^{p-1} + \ldots + a_0$, and the Inversive Congruential Generator with $G(k_{n-1}) = ak_{n-1}^{-1} + c$ [1, 14–17]. Alternatively, we will show that the function G can be obtained by digitizing a chaotic map.

Regardless of the linearity of G, a generator with finite memory like those of the form (1) can be implemented in a finite state machine, being the state of the machine at the time-step n the j-tuple $\sigma_n = (k_{n-1}, \ldots, k_{n-j}) \in \Sigma = \Lambda_n^j$. Since the cardinality of Σ is finite and due to the deterministic nature of the machine evolution, for any initial seed $\sigma_0 \in \Sigma$ the sequence $\{\sigma_i, i \in \mathbb{N}\}$ is eventually periodic with period $\mu(\sigma_0)$, and it enters the loop after a transient of $\eta(\sigma_0)$

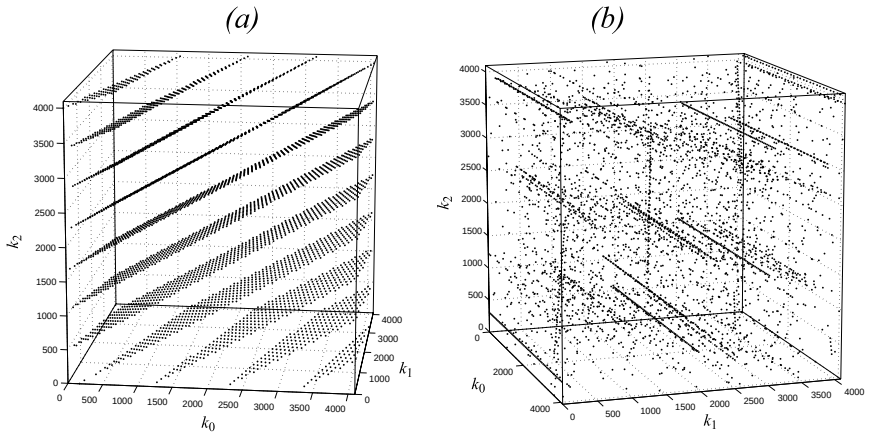


Figure 1: The distribution of vectors (k_2, k_1, k_0) for the linear congruential generator $k_n = 1333k_{n-1} + 3 \bmod 2^{12}$ (subplot (a)) and for the nonlinear congruential generator $k_n = k_{n-1}^3 - k_{n-1}^2 + 7 \bmod 2^{12}$ (subplot (b)).

steps [10]. As a result, the same happens to the sequences of pseudo-random numbers, being the generated number at the time-step n dependent of the state σ_n. A generator that for any σ_0 generates a sequence with period equal to the cardinality of Σ is called a maximum cycle generator.

The problem of relating the length of the cycles μ with the initial seed σ_0 and the generator parameters (e.g., for a linear generator the coefficients in the linear combination G), is an issue of high interest in cryptography. Indeed, it is desirable to know *a priori* that a given sequence of pseudo-random numbers will not enter a too-short predictable cycle. For generators based on linear recurrences the problem has been studied in depth, and well known design criteria are at disposal to obtain maximum cycle devices. On the other hand, for most families of nonlinear generators the problem seems to be intractable, with few exceptions [1, 18].

When dealing with cryptographic applications, linear methods for generating pseudo-random sequences (like LFSRs, LCGs or their proper combinations) are highly not recommended, since efficient algorithms are at disposal to predict the sequence on the basis of a relatively short sequence observation [8, 9]. This cryptographic weakness is reflected by the fact that methods based on linear recurrences may generate numbers lying on regular lattices [19]. In detail, $(d+1)$-tuples of generated numbers $(k_n, k_{n-i_1}, \ldots, k_{n-i_d})$ in the sequence form vectors that belong to a lattice structure in $\mathbb{N}^{d+1}$, as shown in the subplot *(a)* of Fig. 1. In the subplot *(b)* of the same figure it is shown that this does not happen for nonlinear generators, for which the distributions of generated points can reveal irregular structures that – it must be underlined – in most cases are far from being uniformly distributed.

Concluding this brief comparison overview, linear recurrences allow for the definition of maximum cycle generators, with regular distributions of generated numbers (even 'too regular' for some applications [15, 19]), involving very efficient hardware or software implementations, and they are highly not recommended in cryptography [1]. These drawbacks can be overcome by nonlinear

generators, but in this case only for few exceptions maximum cycles generators could be designed [15, 18], their hardware or software implementations are less efficient and the distributions of generated numbers can be particularly not uniform. Nevertheless, as shown in this work, solutions derived from chaotic systems can help in defining nonlinear cryptographic PRNGs with both efficient implementation and good statistical properties.

3 Statistically stable mixing systems

Since our aim is to derive nonlinear congruential generators from certain chaotic maps, in this Section we overview some fundamentals that will be used afterwards. The theory presented hereafter has been simplified to match the aim of this work, adopting the following notation and terminology. With reference to the Lebesgue integration theory, the notation $L^p(I)$ denotes the set of functions $f : I \to \mathbb{R}$ such that $\int_I |f(x)|^p dx < \infty$, with $0 < p \in \mathbb{N}$, whereas $L^\infty(I)$ is the set of almost everywhere bounded measurable functions. We recall that $L^p(I)$ and $L^\infty(I)$ can be made Banach spaces with reference to the norms $\|f\|_p = (\int_I |f(x)|^p dx)^{\frac{1}{p}}$ and $\|f\|_\infty = \inf\{M \in \mathbb{R}^+ \text{ such that } \{x \in I : |f(x)| > M\} \text{ has zero measure}\}$, respectively. We define Π as the set of all finite partitions of intervals of $[0, 1)$, i.e., if $Q \in \Pi$ then $Q = \{I_i, i = 1, \ldots, q, \text{with } q > 0\}$, with $I_i \cap I_j = \varnothing$ for $i \neq j$ and $\cup_{i=1}^{q} I_i = [0, 1)$. Among the elements of Π we highlight the partition $\mathcal{P}_n = \{I_0, \ldots, I_{2^n-1}\}$ made of the 2^n equal and disjoint intervals that divide $[0, 1)$.

We define the special set of probability density functions (pdfs) of bounded variations [20] as

$$D_{BV} = \{f \in L^1([0, 1)) : \|f\|_1 = 1, f \geq 0, f \text{ is of bounded variation}\}. \quad (2)$$

The set D_{BV} is a wide set containing all those pdfs of practical interest and physical meaning.

The chaotic systems taken into account in this work are those ruled by the maps defined as in the following

Definition 1 *The map $S : [0, 1) \to [0, 1)$ is piecewise affine expanding (PWAE) if and only if it is onto and there exists a partition $Q \in \Pi$, with $Q = \{I_0, \ldots, I_{q-1}\}$, such that $S|_{I_i}$ is a linear function of the form $S|_{I_i}(x) = \gamma_i x + \beta_i$, with $\gamma, \beta_i \in \mathbb{R}$ and $|\gamma_i| > 1$ $(i = 0, \ldots, q - 1)$.*

3.1 Statistical stability and correlation decay

We say that a pdf $\phi^* \in L^1$ is invariant for the map S if for any subset $A \subseteq [0, 1)$ it results

$$\int_A \phi^*(x)dx = \int_{S^{-1}(A)} \phi^*(x)dx,$$

which implies $P(S(x) \in A) = P(x \in A)$. By assuming $x_0 \in [0, 1)$ as a random variable with pdf ϕ_0, let us focus on the sequence $\{S^p(x_0), p \in \mathbb{N}\}$. Even if S is deterministic $x_p = S^p(x_0)$ is a stochastic variable and we denote with ϕ_p its associated pdf. In this paper we refer to the following

Definition 2 *A PWAE map S is said to be statistically stable if $\forall \phi_0 \in D_\Pi$ there exists an unique invariant pdf $\phi^* \in L^1([0,1))$ such that*

$$\lim_{p\to\infty} \|\phi_p - \phi^*\|_\infty = 0. \tag{3}$$

According to the above definition, for a statistically stable PWAE map as far as $p \to \infty$ the pdf of the random variable $S^p(x_0)$ approaches an invariant (stationary) pdf ϕ^* that only depends on the map S, regardless of the distribution of the initial condition x_0. The evolution of densities $\{\phi_p, p \in \mathbb{N}\}$ can be analyzed by means of the Frobenious-Perron operator $\Theta_S : D_\Pi \to D_\Pi$

$$\phi_{p+1} = \Theta_S \phi_p(x) = \sum_{y=S^{-1}(x)} \frac{\phi_p(y)}{\left|\frac{dS}{dy}(y)\right|}. \tag{4}$$

An efficient numerical method for analyzing the convergence rate of the sequence of pdfs can be found in [21,22]. As shown in the next sections, in practical cases that are of interest for random number generation the transient (3) vanishes in few steps.

A consequence of statistical stability is the decay of the autocorrelation function associated to the stochastic process $\{S^p(x_0), p \in \mathbb{N}\}$ [23]. Once assuming the process stabilized on its invariant density ϕ^* the autocorrelation function r_{xx} is given by

$$r_{xx}(m) = E\{xS^m(x)\} = \int_0^1 xS^m(x)\phi^*(x)dx. \tag{5}$$

3.2 True random number generation with Rényi maps

Let us consider a special case of PWAE maps, i.e., the family of Rényi transformations

$$S_\beta(x) = \beta x \bmod 1, \qquad \beta > 1, \beta \in \mathbb{R}, \tag{6}$$

where we assume the modulus operator extended to the real numbers, i.e., $\beta x \bmod 1 = \beta x - \lfloor \beta x \rfloor$. In the following, we denote with $b = \lfloor \beta \rfloor$ the integer part of β, whereas we denote with $\gamma = \beta \bmod 1$ its fractional part. If the parameter β assumes integer values $b \in \mathbb{N}$ (i.e., $\gamma = 0$) the Rényi map has the uniform pdf as its unique stationary pdf [20]. In such case the Frobenious-Perron operator can be explicitly written as

$$\phi_{p+1} = \Theta_{S_b} \phi_p(x) = \frac{1}{b} \sum_{i=0}^{b-1} \phi_p\left(\frac{x+i}{b}\right), \tag{7}$$

and it can be easily used for evaluating the limit (3) starting from an arbitrary pdf ϕ_0. Moreover, since $S_b^m(x) = b^m x \mod 1$, the autocorrelation function (5) results equal to

$$\begin{aligned} r_{xx}(p) &= E\{x_i S_b^p(x_i)\} = \sum_{i=0}^{b^p-1} \int_{\frac{i}{b^p}}^{\frac{i+1}{b^p}} x(b^p x - i)dx = \\ &= \sum_{i=0}^{b^p-1} \left(\frac{(i+1)^3}{2b^{2p}} - \frac{i(i+1)^2}{2b^{2p}} - \frac{i^3}{3b^{2p}} + \frac{i^2}{2b^{2p}} \right) = \frac{3b^p+1}{12b^p}. \end{aligned} \tag{8}$$

According to the previous result, as far as $b^m \to \infty$ the autocorrelation approaches 0.25, i.e., the sequence of numbers $\{x_{km}, k \in \mathbb{N}\}$ becomes a sequence of uncorrelated random variables uniformly distributed in $[0, 1)$. The hyperbolic curve

$$r_{xx}(m) - \frac{1}{4} = \frac{1}{12b^m} \tag{9}$$

represents the correlation decay associated to the chaotic sequence, assuming the chaotic state pdf stabilized on its invariant uniform pdf.

3.2.1 Ideal Random Number Generators

If the Rényi map S_b is stabilized on its invariant uniform pdf, it is possible [20, 24] to generate a sequence $\{\psi_i, i \in \mathbb{N}\}$ of i.i.d. uniform random integers $\psi_i \in \{0, \ldots, b-1\}$ by partitioning the domain with the b intervals

$$J_i = \left[\frac{i}{b}, \frac{i+1}{b}\right), \qquad i = 0, \ldots, b-1, \tag{10}$$

and coding the sequence $\{S_b^i(x_0), i \in \mathbb{N}\}$ with the rule

$$\psi_i = m \Leftrightarrow S_b^i(x_0) \in J_m. \tag{11}$$

The partition made of the intervals (10) is called the *natural generating symbolic partition*.

The above technique defines the way to generate a symbolic sequence from any chaotic trajectory, obtaining an information source of i.i.d. uniformly distributed b random integers, i.e., the above technique defines an ideal TRNG. We recall that for an ideal TRNG having as alphabet the first M nonnegative integers it must result:

$$E\{\psi\} = \sum_{i=0}^{M-1} \frac{i}{M} = \frac{M-1}{2}, \tag{12}$$

and in general, for $k \geq 1$,

$$E\{\psi_{m_1} \ldots \psi_{m_k}\} = \frac{(M-1)^k}{2^k}. \tag{13}$$

It is interesting noting that if we apply the generation rule (11) referring to a symbolic partition made of M intervals that are different from those of the form (10), in general we obtain a Markovian information source that generates sequences biased and affected by memory [4, 20, 24]. In other words, we obtain a not ideal TRNG not satisfying (12) and (13), and we stress that in general the obtained Markovian source can have infinite memory [23, 25].

Nevertheless, since the uniform pdf is the invariant pdf for the Rényi map S_b, the biasing between numbers can be eliminated using a symbolic partition made of intervals with equal length, obtaining (12) to be satisfied. Nevertheless, as shown in the following example, this trick may not help in eliminating the correlation between the generated numbers.

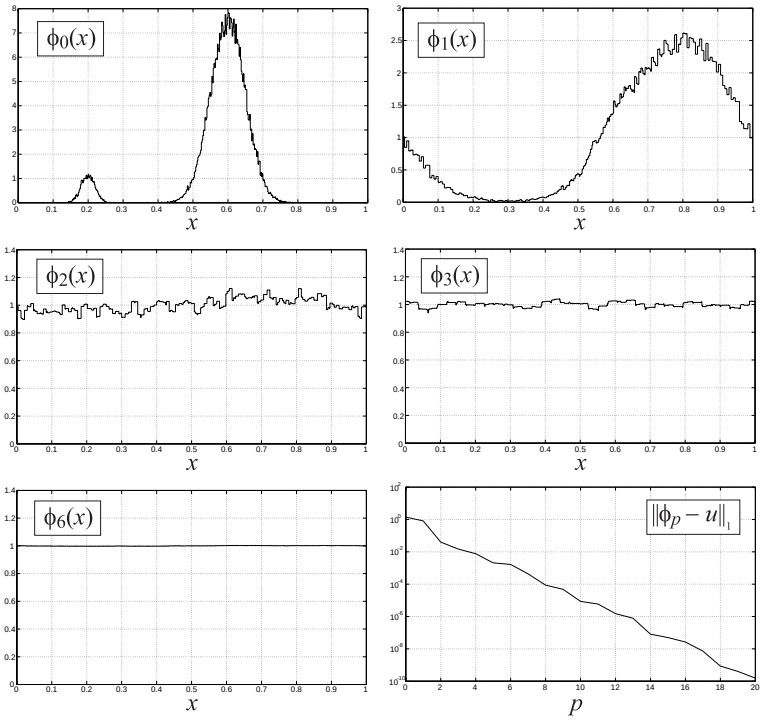


Figure 2: The pdfs associated to the random variables $y = S_3^p(x)$, for $p = 0, 1, 2, 3, 6$. After 6 iterations the distance $\|\phi_5 - u\|_\infty$ is lower than 10^{-3}: the convergence rate is exponential, as confirmed in the log-scale plot of $\|\phi_p - u\|_\infty$. The pdfs were calculated exploiting a modified version of the accurate approach described in [21, 22].

3.2.2 Example

Let us consider the Rényi chaotic map

$$S_3(x) = 3x \bmod 1. \tag{14}$$

If the state x_0 is not uniformly distributed, a vanishing transient occurs for the state pdf to reach the stationary invariant pdf. More in detail, regardless of the pdf $\phi_0 \in D_\Pi$ associated to x, the greater is p and the more the random variable $y = S_3^p(x)$ is uniformly-distributed, as stated in (3). In other words, $\forall \varepsilon > 0$ there exists p such that

$$\|\phi_p - u\|_\infty < \varepsilon, \tag{15}$$

where $u : [0, 1) \to \{1\}$ is the uniform pdf. The number of iterations p necessary to satisfy the above inequality in general depends on ϕ_0 and ε, but *in cases of practical interest*, since the convergence rate is exponential, few iterations suffice to obtain a reasonably accurate approximation of the uniform pdf u [3, 20]. Indeed, 8 iterations of the map S_3 suffices to satisfy the inequality (15) with values of ε in the order of 10^{-4}, even when ϕ_0 is quite different from the uniform pdf (see, e.g., Fig. 2).

As far as the map S_3 is used to define a TRNG, the statistical characteristics of the obtained information source depends on the chosen symbolic partition.

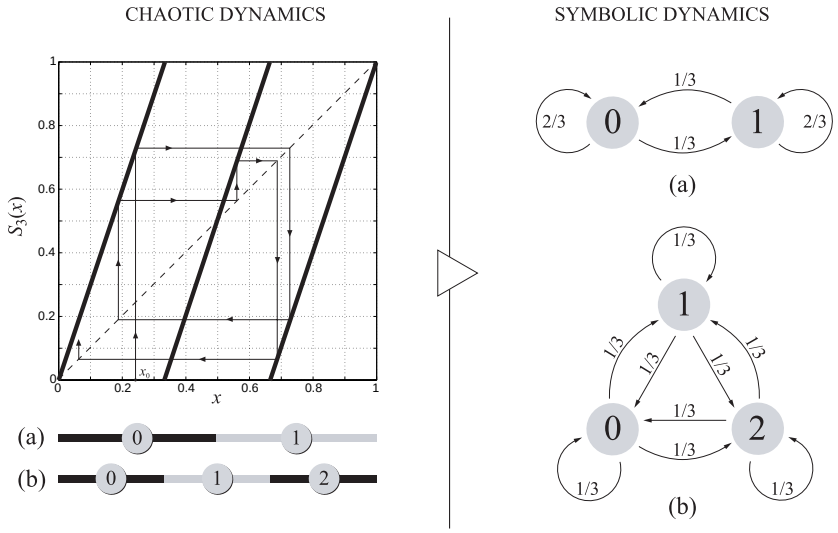


Figure 3: The Rényi map $S_3(x) = 3x \bmod 1$ and the Markov chains modeling the symbolic dynamics obtained by partitioning the domain with the partition $\mathcal{P}_1 = \left\{\left[0, \frac{1}{2}\right), \left[\frac{1}{2}, 1\right)\right\}$– case (a) – and the natural generating symbolic partition $\left\{\left[0, \frac{1}{3}\right), \left[\frac{1}{3}, \frac{2}{3}\right), \left[\frac{2}{3}, 1\right)\right\}$ – case (b). The state transition probabilities of the Markov chains are reported beside the arrows.

To make clear this idea, in Fig. 3, we represented the two Markov chains that model the symbolic dynamics obtained by partitioning the domain $[0, 1)$ with the partition $\mathcal{P}_1 = \left\{\left[0, \frac{1}{2}\right), \left[\frac{1}{2}, 1\right)\right\}$ – case (a) – and the natural generating symbolic partition $\left\{\left[0, \frac{1}{3}\right), \left[\frac{1}{3}, \frac{2}{3}\right), \left[\frac{2}{3}, 1\right)\right\}$ – case (b). In the case (a) the obtained TRNG is not ideal. Indeed, by denoting with I_1 the interval $[\frac{1}{2}, 1)$ we have

$$\begin{aligned} E\{\psi_{m_1} \dots \psi_{m_k}\} &= \sum_{\substack{\psi_{m_1} \in \{0,1\} \\ \dots \\ \psi_{m_k} \in \{0,1\}}} \psi_{m_1} \dots \psi_{m_k} P(\psi_{m_1} \dots \psi_{m_k}) = \\ &= P(\psi_{m_1} = 1, \dots, \psi_{m_k} = 1) = P\left(x \in \bigcap_{i=1}^{k} S_3^{-m_i}(I_1)\right) = \\ &= \int_{\bigcap_{i=1}^{k} S_3^{-m_i}(I_1)} u(x)dx = \lambda\left(\bigcap_{i=1}^{k} S_3^{-m_i}(I_1)\right), \end{aligned} \tag{16}$$

where λ represents the Lebesgue measure. When $k = 1$ in (16), we obtain the mean value

$$E\{\psi\} = \frac{1}{2}, \tag{17}$$

that satisfies (12) for $M = 2$. When $k = 2$ in (16), by denoting with $m = m_2 - m_1$, we obtain the autocorrelation function

$$R_{xx}(m) = E\{\psi_i \psi_{i+m}\} = \frac{1}{4} + \frac{1}{2 \cdot 3^m}, \tag{18}$$

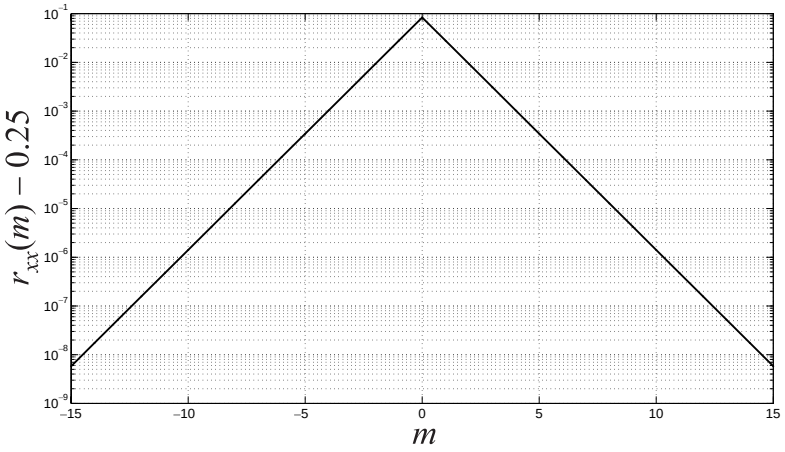


Figure 4: The autocorrelation decay (9) for the sequence $\{S_3^p(x), p \in \mathbb{N}\}$, plotted in logarithmic scale.

that only asymptotically satisfies (13) for $M = 2$, if $m \to \infty$, i.e., if the generated symbols becomes progressively uncorrelated. In general, the same can be shown for any order $k \geq 2$.

On the other hand, when the Rényi map S_3 is partitioned with its natural generating symbolic partition, adopting the same theoretical approach it can be easily shown that the obtained TRNG is ideal: the three integers that may be generated are i.i.d. and their generation probabilities are equal to 1/3, with a k-th order joint probability $P(\psi_1, \psi_2, \ldots, \psi_k) = \prod_{i=1}^{k} \frac{1}{3} = \frac{1}{3^m}$, satisfying both (12) and (13) for any order k.

It is worth noting that the result (18) is in accordance with the correlation decay property (9) between x and $S_3^m(x)$. Indeed, it is expected that if x and $S_3^m(x)$ are not correlated, also the two numbers generated with the rule (11) are not correlated. The autocorrelation function depicted in Fig. 4 shows that a few under-sampling steps suffice to have a negligible residual correlation between x and $S_3^m(x)$.

3.2.3 Preliminary conclusions

The above discussion lead to two different strategies for generating random numbers with the chaotic Rényi maps:

A) To divide the domain $[0, 1)$ with the natural generating symbolic partition associated to the map S_b, in order to obtain an *ideal* TRNG issuing b random integers;

B) To divide the domain $[0, 1)$ with an arbitrary partition $\mathcal{P}_n$ of 2^n intervals, in order to obtain a *not-ideal* TRNG issuing 2^n random integers. In such case the symbols are uniformly distributed, but they are affected by a correlation of any order that has a vanishing decay. Accordingly, an ideal TRNG issuing 2^n random integers can be approximated with any accuracy by under-sampling the sequence $\{S_b^i(x), i \in \mathbb{N}\}$ by a factor p, that is referring to the sequence $\{S_b^{ip}(x), i \in \mathbb{N}\}$.

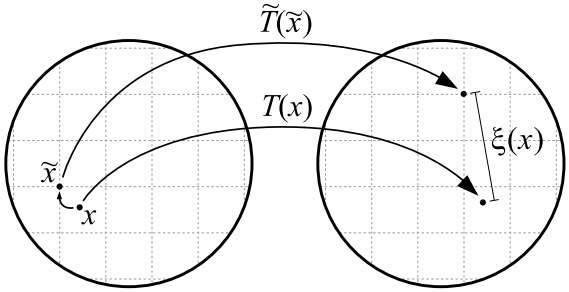


Figure 5: The effect of the finite-precision computation of a generic function T.

Furthermore, we stress that if b can be divided by q, then b/q unions of q partitioning intervals can be used to obtain an ideal TRNG that can generate random integers in the set $\{0, \ldots, b/q\}$. For example, any Rényi map S_b with b even can be used to define an ideal TRNG with alphabet $\{0, 1\}$, referring to the partition $\mathcal{P}_1$. The process is similar to generating even or odd numbers throwing a fair six-sided die.

4 Pseudo-Chaotic Systems

In this work we propose to exploit the ergodic dynamics of PWAE chaotic maps for the design of nonlinear PRNGs with good statistical properties and that involve low-complexity implementations. To this aim, we start analyzing the links that exist between chaos and pseudo-chaos. Pseudo-chaos is obtained when a chaotic dynamical system is simulated using finite precision arithmetic algorithms [26–28]. In detail, referring to a generic chaotic map $T : [0, 1) \to [0, 1)$, the pseudo-chaotic approximation of T is obtained in two steps. In the first step any point $x \in [0, 1)$ is represented by a finite-precision point $\tilde{x}$ belonging to a finite set $\Lambda \subset [0, 1)$, called the discrete domain. Accordingly we have the definition of the finite-precision point $\tilde{x} : [0, 1) \to \Lambda$, as a function of x. In the second step the function T is approximated by a finite-precision approximating function $\tilde{T} : \Lambda \to \Lambda$ such that

$$\left| T(x) - \tilde{T}(\tilde{x}) \right| = \xi(x) < 1, \tag{19}$$

where the function ξ quantifies the quality of the approximation. Summarizing, the overall pseudo-chaotic approximation is defined by the composition $\tilde{T} \circ \tilde{x} : [0, 1) \to \Lambda$. If the function ξ assumes reasonably small values for all x, it is often said that $\tilde{T}$ 'shadows' T.

Trying to relate the properties of the two systems T and $\tilde{T}$ can be a difficult task, depending on their nonlinear functional forms. For example, adopting a dynamical evolution point of view, Coomes et al. in [13] proved some major results valid for hyperbolic diffeomorphisms, that represent a fundamental reference within the Shadowing Theory for chaotic systems. We adopt a different point of view, since we are interested in relating the probability measures associated to T and $\tilde{T}$. In detail, for a given subset $I \subseteq [0, 1)$, we are interested in

the quantity

$$\mathcal{E}(I,\xi) = \left| P(T(x) \in I) - P(\tilde{T}(\tilde{x}) \in I) \right|, \tag{20}$$

where the set I is understood to be a sub-interval of $[0,1)$. Since T is measurable, the previous quantity can be also written as

$$\mathcal{E}(I,\xi) = \left| P(x \in T^{-1}(I)) - P(\tilde{x} \in \tilde{T}^{-1}(I \cap \Lambda)) \right|. \tag{21}$$

Due to the calculating approximation, in general it can happen that

$$\tilde{T}^{-1}(I \cap \Lambda) - (T^{-1}(I) \cap \Lambda) \neq \varnothing, \tag{22}$$

i.e., there are points mapped in I by the function $\tilde{T}$ that do not belong to $T^{-1}(I)$. About this issue, we have the following

Proposition 1 (Proved in [29]) *Let $I \subseteq [0,1)$ be an interval with endpoints $a < b$, and let us assume that $\forall x \in T^{-1}(I)$ it results*

$$\left| T(x) - \tilde{T}(\tilde{x}) \right| < \alpha = \sup_{x \in T^{-1}(I)} \xi(x). \tag{23}$$

Accordingly, by denoting with ϕ the pdf of $T(x)$, if $b - a \geq 2\alpha$ then it results

$$\int_{a+\alpha}^{b-\alpha} \phi(x)dx \leq P\left(\tilde{T}(\tilde{x}) \in I\right) \leq \int_{a-\alpha}^{b+\alpha} \phi(x)dx. \tag{24}$$

It is worth noting that the above Proposition has a general validity, and that if the condition (23) holds in the whole interval $[0,1)$, then the result (24) holds for any interval $I \subseteq [0,1)$ with length greater than 2α. This is the case provided by the Shadowing Theory, that is valid for certain continuous maps [13]; in this work we allow the chaotic map to be *not* continuous, as discussed in the following.

4.1 Almost-uniform measure-preserving chaotic transformations

Under the hypotheses of Proposition 1, in this subsection we refine the theoretical result (24) assuming the random variable $T(x)$ almost uniformly-distributed, i.e., we assume

$$\|\phi - u\|_\infty \leq \varepsilon,$$

where $u : [0,1) \to \{1\}$ is the uniform pdf over $[0,1)$. Accordingly, for any interval $I \subseteq [0,1)$ with endpoints $a < b$ it results

$$(b-a)(1-\varepsilon) \leq \int_I \phi(x)dx \leq (b-a)(1+\varepsilon). \tag{25}$$

If we now assume the interval I to have Lebesgue measure $\frac{1}{2^k}$, i.e., $b - a = \frac{1}{2^k}$, using (25) the inequality (24) can be rewritten as

$$\left(\frac{1}{2^k} - 2\alpha\right)(1-\varepsilon) \leq P\left(\tilde{T}(\tilde{x}) \in I\right) \leq \left(\frac{1}{2^k} + 2\alpha\right)(1+\varepsilon),$$

which implies

$$-\frac{\varepsilon}{2^k} - 2\alpha(1-\varepsilon) \leq P\left(\tilde{T}(\tilde{x}) \in I\right) - \frac{1}{2^k} \leq \frac{\varepsilon}{2^k} + 2\alpha(1+\varepsilon).$$

Focusing on the worst case, we finally have

$$\left| P\left(\tilde{T}(\tilde{x}) \in I\right) - \frac{1}{2^k} \right| \leq \frac{\varepsilon}{2^k} + 2\alpha(1+\varepsilon), \tag{26}$$

which leads to the relative error

$$\frac{\left| P\left(\tilde{T}(\tilde{x}) \in I\right) - \frac{1}{2^k} \right|}{\frac{1}{2^k}} \leq \varepsilon + 2^{k+1}\alpha(1+\varepsilon). \tag{27}$$

4.2 Random perturbations

We stress that the above results hold even assuming the function $\tilde{T}$ to be stochastic, i.e., perturbed by a small additive random noise. In such case the quantity $|T(x) - \tilde{T}(\tilde{x})|$ is a random variable, and the Proposition 1 and (26) hold provided to define α as the supremum of $|\xi(x) + \nu|$, being ν the stochastic fluctuation. As it will be made clearer in the following, we will consider pseudo-random perturbations of the pseudo-chaotic map $\tilde{T}$, to make the resulting nonlinear generator immune from short periodic cycles.

5 Nonlinear recurrences derived from the Rényi map

There is an infinite number of different ways to define the digitized version of a chaotic system. In this section we propose a method for digitizing the Rényi maps, in order to obtain PRNGs based on nonlinear recurrences. Assuming $n \in \mathbb{N}$, with $n > 1$, we define the discrete domain as the following set of dyadic rationals

$$\Lambda_{2^n} = \left\{ \frac{q}{2^n} \in \mathbb{Q} : 0 \leq q < 2^n \right\}.$$

Given the Rényi map $S_b(x) = bx \bmod 1$, for any arbitrary small positive $\gamma \ll 1$ we define the digitized map $\tilde{S}_\beta : \Lambda_{2^n} \to \Lambda_{2^n}$ as

$$\tilde{S}_\beta\left(\frac{q}{2^n}\right) = \frac{1}{2^n}\left(\lfloor (b+\gamma)q \rfloor \bmod 2^n\right) = \frac{1}{2^n}\left(bq + \lfloor \gamma q \rfloor \bmod 2^n\right) \tag{28}$$

The link between x and $\tilde{x}$ is defined assuming the truncation strategy to approximate x, i.e., if $x \in [0,1)$ it results

$$\tilde{x} = \frac{q(x)}{2^n} = \frac{\lfloor 2^n x \rfloor}{2^n}. \tag{29}$$

Accordingly, any point x can be written as $x = \tilde{x} + \xi(x) = \frac{q(x)}{2^n} + \xi(x)$, where $\xi(x) \in [0, 2^{-n})$. Summarizing, S_b and $\tilde{S}_b$ are linked by the definition rules shown in Fig. 6. We spend few words on the role of the above introduced parameters γ and n. First of all, we stress that the digital architecture implementing

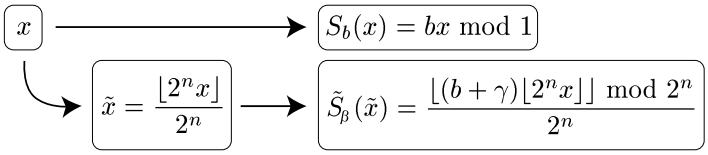


Figure 6: The definition rules for the pseudo-chaotic Rényi map.

(28) is a n-bit state machine, and for this reason we call the parameter n the digital resolution of the pseudo-chaotic system [28, 30]. Furthermore, it can be noticed that due to the modular calculations in (28) for any integer b the pseudo-chaotic version of $S_b(x) = bx \bmod 1$ agrees with the pseudo-chaotic version of $S_{b+2^n}(x) = (b+2^n)x \bmod 1$ (for a same value of γ in (28)). Moreover, it must be highlighted that if $0 \leq \gamma < \frac{1}{2^n-1}$ then for any $0 \leq q < 2^n$ the quantity $\lfloor \gamma q \rfloor$ is equal to zero: in such case the expression (28) defines a linear congruential generator. Accordingly, in order to make (28) a nonlinear congruential generator it must be

$$\frac{1}{2^n - 1} \leq \gamma \ll 1. \tag{30}$$

As it will be shown in the next Section, adopting the point of view discussed in Section 4 the greater are n and $1/\gamma$ and the better the dynamics of S is shadowed by $\tilde{S}$.

5.1 Properties of the Digitized Rényi Maps

In this Section we theoretically discuss some of the relationships that exist between the Rényi chaotic maps and their pseudo-chaotic versions (28). We face this problem in two steps. First, we discuss the link between the Rényi map $S_\beta = (b+\gamma)x \bmod 1$ and the Rényi map $S_b(x) = bx \bmod 1$, and then we analyze how (28) approximates $S_b(x)$.

Accordingly, let us begin to analyze the link between S_β and S_b. Referring to the Figs.7 and 8, it can be noticed that the higher absolute error $|S_\beta(x) - S_b(x)|$ is made around the discontinuity points of the maps, i.e., within the union of intervals

$$M = \bigcup_{i=1}^{b} \left[\frac{i}{\beta}, \frac{i}{b} \right). \tag{31}$$

The length of the i-th of these intervals is $i \cdot \Delta$, where $\Delta = \frac{\beta - b}{\beta b}$, and it can be easily verified that the absolute error in $[0,1)/M$ is not greater than $b\left(1 - \frac{b}{\beta}\right)$. Despite the effects of the discontinuities, for small values of γ the dynamics of $S_\beta(x)$ and $S_b(x)$ within a limited time period follow trajectories that are close to each other for most values of x, in the sense specified by the following

Theorem 1 *Let us consider the interval*

$$K_1 = [0, 1 - \delta_1),$$

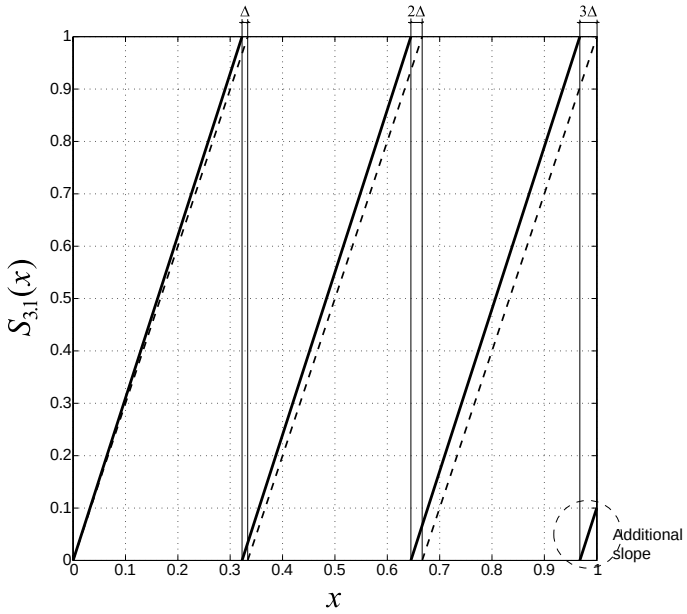


Figure 7: The Rényi map $S_{3.1}$ (solid line) and the Rényi map S_3 (dashed line).

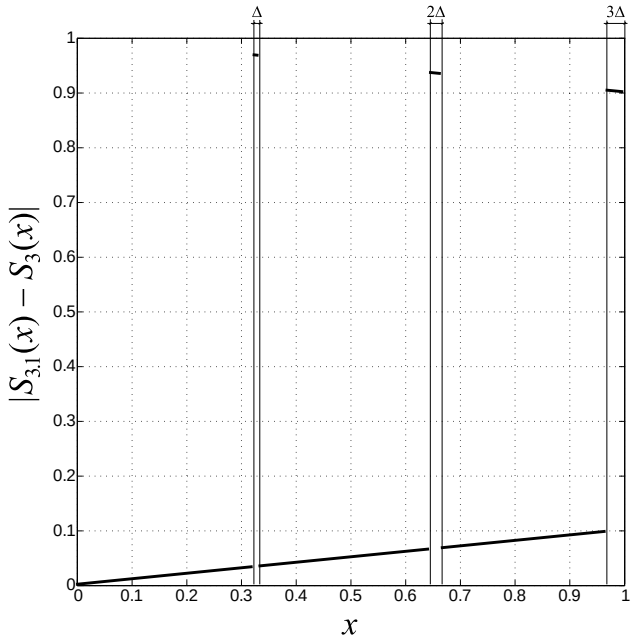


Figure 8: The absolute error $|S_{3.1}(x) - S_3(x)|$ between the two Rényi maps $S_{3.1}$ and S_3.

where $\delta_1 = \left(1 - \frac{b}{\beta}\right) \frac{b^{p+1} - b}{b-1}$ *and* $p \in \mathbb{N}$. *For any* $x \in S_b^{-p}(K_1)$ *it results*

$$\left|S_\beta^p(x) - S_b^p(x)\right| \leq \left(1 - \frac{b}{\beta}\right) \frac{b^{p+1} - b}{b-1}. \tag{32}$$

For proving the theorem, we first need the

Lemma 1 *Let us consider two points* x_1, x_2 *belonging to the same interval* $I = [\frac{i}{b}, \frac{i+1}{\beta})$, *with* $0 \leq i \leq b$. *Accordingly the two points do not belong to* M *and the two maps* S_b *and* S_β *have constant slope in* I. *It results*

$$|S_\beta(x_1) - S_b(x_2)| \leq b|x_1 - x_2| + b\left(1 - \frac{b}{\beta}\right). \tag{33}$$

Proof. We have $|S_\beta(x_1) - S_b(x_2)| = |S_\beta(x_1) - S_b(x_1) + S_b(x_1) - S_b(x_2)| \leq |S_\beta(x_1) - S_b(x_1)| + |S_b(x_1) - S_b(x_2)|$. The first term is not greater than the maximum absolute error $|S_\beta(x) - S_b(x)|$ in $[0,1)/M$, that is $b\left(1 - \frac{b}{\beta}\right)$. On the other hand, since S_b is linear over I, we have $|S_b(x_1) - S_b(x_2)| = b|x_1 - x_2|$, and the lemma is proved. □

We can now prove the Theorem 1.

Proof of Theorem 1. Let us assume that the two points $S_\beta^j(x)$ and $S_b^j(x)$ for $j = 0, 1, \ldots, p-1$ belong to same intervals $I_j = [\frac{i_j}{b}, \frac{i_j+1}{\beta})$, with $0 \leq i_j \leq b$. From the previous Lemma we have

$$\left|S_\beta^{j+1}(x) - S_b^{j+1}(x)\right| \leq b\left|S_\beta^j(x) - S_b^j(x)\right| + b\left(1 - \frac{b}{\beta}\right),$$

and proceeding by induction it is easy to prove that for $j > 0$

$$\left|S_\beta^j(x) - S_b^j(x)\right| \leq \left(1 - \frac{b}{\beta}\right) \sum_{r=1}^{j} b^r = \left(1 - \frac{b}{\beta}\right) \frac{b^{j+1} - b}{b-1}. \tag{34}$$

The above inequality agrees with (32) by setting $j = p$, and the proof is completed if we show that if $x \in S_b^{-p}(K_1)$ then the two points $S_\beta^j(x)$ and $S_b^j(x)$ for $j = 0, 1, \ldots, p-1$ belong to same intervals $I_j = [\frac{i_j}{b}, \frac{i_j+1}{\beta})$, with $0 \leq i_j \leq b$.

Accordingly, we define the set $P_b = \{\frac{i}{b}, 0 < i \leq b\}$ and we note that for $j = 0$ the previous condition is satisfied if the distance of x from the greater nearest point in P_b is not smaller than $(1 - \frac{b}{\beta})$: this is a sufficient condition for x not to belong to the set M defined in (31). For the second step, since we know from (34) that $|S_\beta(x) - S_b(x)| < b(1 - \frac{b}{\beta})$, a sufficient condition to have both of the points $S_\beta(x), S_b(x)$ in a same interval I_1 is to have $S_b(x)$ not closer than $b(1 - \frac{b}{\beta}) + (1 - \frac{b}{\beta})$ to the greater nearest point in P_b. Generalizing, for $j = 0, \ldots, p-1$ both of the points $S_\beta^j(x), S_b^j(x)$ lye in a same interval I_j if $S_b^j(x)$ is not closer than

$$\left(1 - \frac{b}{\beta}\right) \sum_{r=0}^{j} b^r = \left(1 - \frac{b}{\beta}\right) \frac{b^{j+1} - 1}{b-1}$$

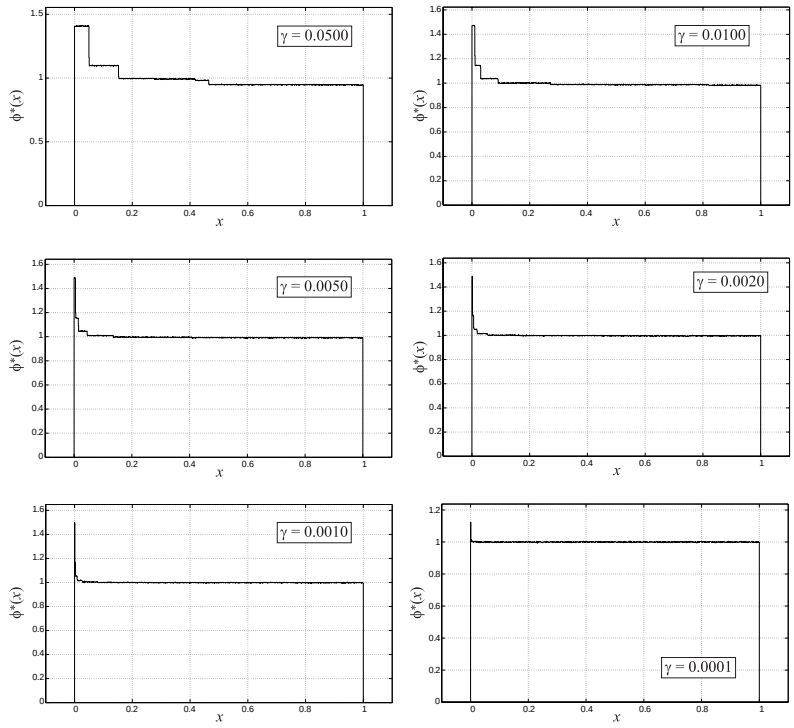


Figure 9: The estimation of the invariant pdf for the Rényi maps $S_{3+\gamma}$, for several values of γ. From the Ergodic Theory of dynamical systems it results $\lim_{\beta\to b}\left\|\phi^*_\beta - u\right\|_1 = 0$, where u is the uniform pdf in $[0,1)$ [20, 21].

to the greater nearest point in P_b.

Let us now focus on the set K_1: we will show that for $m = 1,\ldots,p$ the set $S_b^{-m}(K_1)$ contains only points that satisfy the previous sufficient conditions. In detail, we note that the set $S_b^{-1}(K_1)$ is made of b intervals of the form $[\frac{i}{b}, \frac{i}{b} + \frac{1-\delta_1}{b})$ for $0 \le i < b$, that is, each point in $S_b^{-1}(K_1)$ is not closer than $\frac{\delta_1}{b}$ to the greater nearest point in P_b. Following the same reasoning, it is easy to check that each point in $S_b^{-m}(K_1)$ is not closer than $\frac{\delta_1}{b^m}$ to the greater nearest point in P_b. Accordingly, in order to satisfy the previously discussed sufficient conditions, it suffices that

$$\frac{\delta_1}{b^{p-j}} \ge \left(1 - \frac{b}{\beta}\right)\frac{b^{j+1}-1}{b-1}, \tag{35}$$

that is satisfied for $j = 0,\ldots,p-1$ if

$$\delta_1 = (1 - \frac{b}{\beta})\frac{b^{p+1}-b}{b-1}, \tag{36}$$

concluding the proof. □

The previous result indicates that for any $p \in \mathbb{N}$ if $\gamma \to 0$ the trajectory of $\{S_\beta^j(x)\}$ converges to the trajectory $\{S_b^j(x)\}$ uniformly over $\{0,\ldots,p\}$. Moreover, we stress that the invariant measure induced by the uniform pdf of the

Rényi map S_b agrees with the Lebesgue measure of intervals, and in such case the Lebesgue measure of $S_b^{-p}(K_1)$ is equal to $1-\delta_1$. Accordingly, for $\gamma \to 0$ δ_1 goes to zero and the property (32) holds almost everywhere in $[0,1)$.

This fact is somehow reflected by the shape of the invariant pdf associated to S_β. In detail, the Ergodic Theory [7,20] provides the tools for showing that

$$\lim_{\beta \to b} \left\| \phi_\beta^* - u \right\|_1 = 0, \tag{37}$$

i.e., the invariant pdf associated to S_β converges in $L^1([0,1))$ to the invariant pdf of S_b, that is the uniform pdf. As it can be seen in Fig. 9, the presence of the additional slope highlighted in Fig. 7 causes an accumulation of the pdf around the point 0, and the effect vanishes as soon as γ goes to zero. A rigorous theoretical approach to analyze this topic and to demonstrate the above limit is reviewed and discussed in [20,21].

As a second step of our analysis, we investigate the link between $\tilde{S}_\beta$ and S_b. The procedure is similar to that one previously discussed, with the difference that we have to take into account, defining the map $\tilde{S}_\beta$, the effects of the truncations. In detail, we have the following

Theorem 2 *Let us consider the interval*

$$K_2 = [\delta_2, 1-\delta_2)\,,$$

with

$$\delta_2 = \frac{2\beta^{p+1}}{(\beta-1)2^n} + \left(1+\frac{b}{\beta}\right)\frac{b^{p+1}-b}{b-1}, \tag{38}$$

and $p, n \in \mathbb{N}$. For any $x \in S_b^{-p}(K_2)$ it results

$$\left| S_b^p(x) - \tilde{S}_\beta^p(\tilde{x}) \right| < \frac{\beta^{p+1}-1}{(\beta-1)2^n} + \left(1-\frac{b}{\beta}\right)\frac{b^{p+1}-b}{b-1}. \tag{39}$$

Proof. See the Appendix.

The previous theorem represent the main result of this work, since it explicitly relates the dynamics of the pseudo-chaotic map $\tilde{S}_\beta$ with the dynamics of the original chaotic Rényi map S_b. Interestingly, we highlight two aspect. First, by increasing n the effect of the digitization vanishes exponentially. Moreover, we recall from the discussion at the beginning of this Section that to have a nonlinear congruential generator the parameter $\gamma = \beta - b$ must be not smaller than $\frac{1}{2^n-1}$. Accordingly, the larger is n and the more the parameter β can be set close to b. The larger is n, the more β can be set close to b and the more the interval K_2 covers the entire domain. Accordingly, by playing with n and β one can design a pseudo-chaotic map whose dynamics is arbitrarily close the the original chaotic Rényi map S_b, obtaining nonlinear recurrences.

5.1.1 Example

Let us consider the Rényi map S_3, and let us define its digitization by means of the 32 bit pseudo-chaotic map

$$\tilde{S}_{3+\gamma}\left(\frac{m}{2^{32}}\right) = \frac{1}{2^{32}}\left\lfloor (3+\gamma)m \bmod 2^{32} \right\rfloor, \tag{40}$$

where $\gamma = 6.886664777994155883789062 5 \cdot 10^{-6}$ and $\beta = \texttt{0x3.0000738A}$. Adopting the binary fixed point representation, β can be written as

$$11.0000\ 0000\ 0000\ 0000\ 0111\ 0011\ 1000\ 1010. \tag{41}$$

As discussed in the next Section, the binary representation of β plays a key-role to determine the computation complexity involved by the PRNG based on the pseudo-chaotic Rényi maps. From Theorem 2 we have that

$$\begin{aligned}\left|S_3^p(x) - \tilde{S}_{3+\gamma}^p(\tilde{x})\right| &\leq \frac{(3+\gamma)^{p+1}-1}{(3+\gamma)2^{32}} + \left(1 - \frac{3}{3+\gamma}\right)\frac{3^{p+1}-3}{2} \approx \\ &\approx \begin{cases} 2.328 \cdot 10^{-10}, & \text{if } p = 0, \\ \vdots & \\ 2.755 \cdot 10^{-5}, & \text{if } p = 2, \\ \vdots & \\ 7.528 \cdot 10^{-3}, & \text{if } p = 7 \ldots \end{cases}\end{aligned} \tag{42}$$

The above inequalities hold for any point x such that $S^p(x) \in K_2 \approx [0.0075, 0.9925)$, that is calculated for $p = 7$. As a result, if we set $T = S_3^7$ and $\alpha = 7.528 \cdot 10^{-3}$, referring to the partition $\mathcal{P}_3$, from (27) we obtain that for any interval I_j of the partition that also belongs to K_2

$$\frac{\left|P\left(\tilde{T}(\tilde{x}) \in I_j\right) - \frac{1}{8}\right|}{\frac{1}{8}} \leq \varepsilon + 16 \cdot 7.528 \cdot 10^{-3}(1+\varepsilon). \tag{43}$$

If we assume ε in the order of 10^{-3} (i.e., according to a worst case indicated by the numerical analysis, see Fig. 2), the above inequality yields that the probability for the state $\tilde{x}$ to belong to any interval $I_j \subset K_2$ of the partition $\mathcal{P}_3$ after 7 iterations of the digitized Rényi map differs from 1/8 by a relative error that is smaller than 12%, even if, in the worst case, the distribution of the initial state was very different from the uniform distribution. If the initial state is better uniformly distributed, the number of iterations decreases and the bounds decrease exponentially.

Theorem 2 does not tell us what may happen outside the interval K_2, at the borders of the phase space $[0, 1)$: if $x \notin T^{-p}(K_2)$ the 'shadowing error' made by the digitized map $\tilde{T}$ after p iterations can be much greater than the upper bound (24), due to the effects of the map discontinuities. Actually, in practical cases this fact has negligible consequences on the short-term statistical behavior of the digitized map, since its dynamics is typically observed adopting a coarse-grained resolution, greater than α (e.g., in this example we adopted an observation interval with length 1/8, being α in the order of 10^{-3}).

Nevertheless, we stress that our point of view is statistical: we are not interested in following trajectories exactly; rather, we are interested in emulating the long-term statistical behavior of the original system. To this aim, we must introduce the pseudo-random perturbation of the digitized state trajectories, in order to emulate the trajectory instability of chaotic systems and to avoid the digitized system entering periodic stable orbits.

5.2 Pseudo-random perturbation of digitized chaotic systems: setting the period length

It is well known that periodic trajectories are dense in chaotic attractors [31]. However, they are instable and the probability for a chaotic motion to enter a periodic orbit is zero. That is not what happens in a digitized system, for which all the trajectories are eventually periodic. In this work we propose to emulate the instability of chaotic trajectories by pseudo-randomly perturbing the digitized state $\tilde{x}$. To this aim, we remark that if the perturbation magnitude remains particularly small the shadowing property previously discussed still holds, as highlighted in Section 4.2.

Referring to the approach of Lasota in [25] the presence of noise in a chaotic system can be modeled as it follows. At each time step the chaotic sample x_{p+1} deviates from its ideal value due to a statistically independent noise ν_p added to the sample x_p, i.e.,

$$x_{p+1} = T(x_p + \nu_p). \tag{44}$$

As a result, in a chaotic system the presence of noise can cause the trajectories to diverge, e.g., bringing the perturbed state $x_p + \nu_p$ outside the basin of attraction of the chaotic attractor: this is not the case for a chaotic map like the Rényi map, defined as in (6). In general, the resulting process describes a discrete-time random walk in the phase space $[0, 1)$, that may not admit a stable stationary probability density function [25]. If the noisy samples $\{\nu_p\}$ are i.i.d. random variables statistically independent from the $\{x_m\}$ samples, it results that

$$\phi_{p+1} = \tilde{\Theta}_T(\phi_p \otimes f_\nu), \tag{45}$$

where f_ν is the pdf associated to the noisy samples, whereas the operator $\tilde{\Theta}_T$ is the extension of the Frobenius Perron operator Θ_T defined in (4) to the whole set of densities of bounded variations in $L^1([0, 1))$. It is worth noting that x_p only depends on the noisy samples $\nu_{p-1}, \nu_{p-2}, \ldots$ and if $\phi = \tilde{\Theta}_T(\phi \otimes f_\nu)$ then the pdf ϕ is stationary and invariant for the stochastic dynamical system (44). The characterization of the evolution of densities induced by (45) for systems like (44) is still an open theoretical problem, and depending on the considered case even the existence of an invariant density can be an undetermined issue [25,32]. Nowadays, the consequence of the stochastic perturbations on the dynamics is typically studied resorting to 'computer simulations', and this is exactly what we do by digitizing the Rényi map and by adding a small perturbation noise to the digitized state.

Since our aim is to reproduce the instability of chaotic trajectory, we set the noise magnitude as small as possible, i.e., equal to the digitized resolution $1/2^n$. Accordingly, as discussed in the following Section, we perturb the less significant bit (LSB) of the digitized state $\tilde{x}$ by performing the XOR operation with the output bit of a LFSR. Simulation results show that the chief statistical behavior of the original Rényi map are preserved (See, e.g., Fig. 10).

Even considering the pseudo-random perturbation, the resulting overall computing method is deterministic and the digitized dynamics is still eventually periodic with a period length that can be set greater than a minimum, according to the following

Proposition 2 *Let us consider the binary periodic sequences $y(p)$, $z(p)$ and*

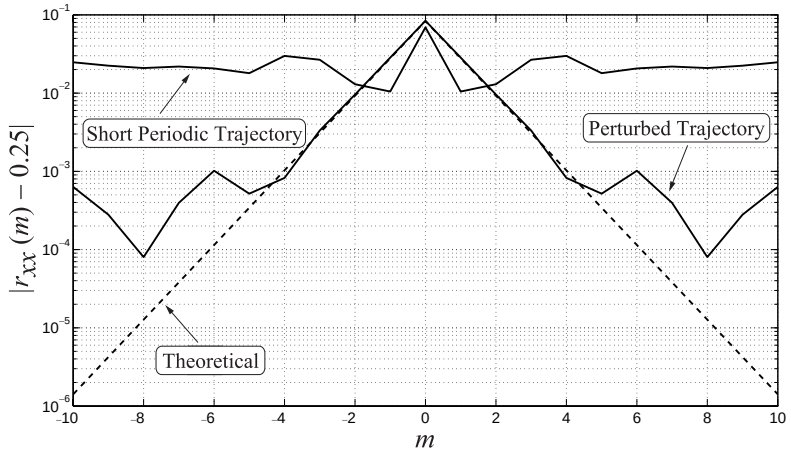


Figure 10: The effect on the correlation decay of the LSB perturbation. The two trajectories were obtained using the digitized map (40), starting from the same initial condition. The autocorrelation functions were estimated on 100000 samples.

$w(p) = y(p) \oplus z(p)$, for $p \in \mathbb{N}$, and let P_y, P_z, P_w be their respective periods. If $P_z > 1$ is prime, then $P_w = kP_z$, with $m \geq 1$.

Proof. Since $P_z > 1$, it is immediate to verify that $P_w > 1$. If $P_w < P_yP_z$ an integer q exists such that $P_yP_z = qP_w + P_yP_z \bmod P_w$, with $0 \leq P_yP_z \bmod P_w < P_w$. On the other hand, $w(p) = y(p) \oplus z(p) = y(p + P_yP_z) \oplus z(p + P_yP_z) = w(p + P_yP_z) = w(p + qP_w + P_yP_z) = w(p + P_yP_z \bmod P_w)$. Since P_w is the smallest integer such that $w(p) = w(p + P_w)$, it must be $P_yP_z \bmod P_w = 0$. Accordingly it results $P_yP_z = hP_w$, that is $P_w = \frac{P_yP_z}{h}$. If P_z is prime, h divides P_y and $P_w = mP_z$. □

Referring to the above notation, we can set $w(p)$ as the LSB of $\tilde{x}_p$, $y(p)$ as the less significant bit of $\tilde{S}(\tilde{x}(p-1))$ and $z(p)$ as the output bit of an LFSR. According to the above proposition, if the LFSR has prime period P_z, then the perturbed trajectories of $\tilde{x}$ have period that is not smaller than P_z. By recalling that a LFSR of order k has period $P_z = 2^k - 1$, we remark that P_z is a Mersenne prime if we set $k = 31$ or $k = 61$, obtaining P_z equal to $2147483647 \approx 2.15 \cdot 10^9$ and $2305843009213693951 = 2.3 \cdot 10^{18}$, respectively. These choices assure that the period of the generated digitized sequences can be made long enough for our cryptographic purposes, regardless of the initial condition of the nonlinear recurrence (28).

5.3 On the hardware/software implementation of the digitized Rényi map

We spend few comments about the hardware/software implementation of the digitized Rényi map, noting that the only operations involved in the calculation are 2^n-modular additions (to calculate the multiplication), with a truncation of the result to the n most significant bits. The number of additions is equal to the number of '1' in the binary representation of β, and the addition operations can

be easily performed referring to efficient solutions like carry-save adders [30]. In the example previously discussed, ten 2^n-modular additions suffices.

6 PRNGs derived from the Rényi map: design and testing

When dealing with PRNGs and statistical tests, one point must be clear: for any given PRNGs it is always possible to define a 'never-passing' test. This is because of the deterministic and periodic nature of PRNGs, that always introduces some undesired defects in the statistical characteristics of the generated sequences. Nevertheless, the results discussed in this paper indicate that for any given finite-time statistical test there is an infinite number of PRNGs based on the pseudo-chaotic Rényi map (28) that pass that test. This is because of the two following remarks:

1. with any Rényi chaotic map S_b (with integer b) it is always possible to obtain an ideal TRNG, by adopting a proper symbolic coding of its dynamics [20];
2. by playing with the parameters n and γ one can use a map $\tilde{S}_\beta$ to approximate the chaotic Rényi map S_b according to any arbitrary accuracy over finite time-windows.

The above point 2. can be faced adopting the two different strategies identified in the preliminary conclusions A) and B), discussed in Section 3.2, taking in mind that the *required accuracy of the approximation depends on the target application* (e.g., it depends on the statistical tests taken into account). Before introducing two specific examples related to these two mentioned approaches, it is worth discussing how to perform the domain partitioning.

6.1 Domain partitioning in digitized chaotic systems

The simplest approximated way to generate numbers referring to the rule (11) is to compare the digitized state $\tilde{x}$ with the endpoints of a symbolic partition: in general, up to $M-1$ comparisons are required for a partition made of M intervals. This operation introduces the problem of comparing dyadic rationals, since even the partition endpoints must be represented according to a digitization strategy. For example, the endpoints $1/3$ and $1/6$ of the natural generating symbolic partition of the map S_3 can not be represented adopting a conventional binary fixed point representation of numbers, and the same happens for the endpoints associated to other maps S_b with $b \neq 2^m$.

On the other hand, it is very easy to apply the generation rule (11) when the partition is of the form $\mathcal{P}_k$, i.e., a partition made of 2^k equal intervals. In such case, no comparison is necessary since the most k significant bits of the state $\tilde{x}$ indicate the number of the belonging interval in the partition, i.e., the generated number of the PRNG. Adopting the same reasoning discussed in the preliminary conclusions of the Section 3.2, the partition $\mathcal{P}_k$ can be used without introducing correlation between symbols if b is of the form $q2^k$, with $q \in \mathbb{N}^+$.

6.1.1 PRNGs design – approach (A)

According to the approach A) discussed in Section 3.2, we divide the domain $[0, 1)$ adopting a refinement of the natural generating symbolic partition associated to the map S_b, in order to approximate an *ideal* TRNG issuing b random integers. Since we refer to partitions of the form $\mathcal{P}_k$, we have to digitize maps S_b with $b = m \cdot 2^k$, for any $m \in \mathbb{N}, m > 1$. As an example, in Table 1 we reported the NIST SP800.22 test [12] results for a PRNG based on $\tilde{T} = \tilde{S}_\beta$, with $n = 64$ bits and $\beta =$ `0x4.000000000001838A` ($b = 4$). At each time step the 2 most significant bits of $\tilde{x}$ were output ($\mathcal{P}_k = \mathcal{P}_2$). The minimum pass rate for each statistical test with the exception of the Random Excursion Variant test is approximately 0.960150 for a sample size of 100 binary sequences (2 million bits each). The minimum pass rate for the Random Excursion Variant test is approximately 0.954323 for a sample size = 70 binary sequences (2 million bits each).

6.1.2 PRNGs design – approach (B)

According to the approach b) discussed in Section 3.2, we divide the domain $[0, 1)$ with an arbitrary partition $\mathcal{P}_n$ of 2^n intervals, in order to approximate a *not-ideal* TRNG. In such case the 2^n random integers are uniformly distributed, but they are affected by a correlation that has a vanishing decay. Accordingly, an ideal TRNG issuing 2^n random integers can be approximated with any accuracy by under-sampling the sequence $\{S^i(x), i \in \mathbb{N}\}$ by a factor p, that is referring to the sequence $\{S^{ip}(x), i \in \mathbb{N}\}$. As an example, we report the NIST SP800.22 test results for a PRNG based on $\tilde{T} = \tilde{S}^8_\beta$, with $n = 32$ bits and $\beta =$ `0x7.000000AA0` ($b = 7, p = 8$). Referring to the map $\tilde{T}$, at each time step the 8 most significant bits of $\tilde{x}$ were output ($\mathcal{P}_k = \mathcal{P}_8$). The tests were performed on a sample size of 100 binary sequences (2 million bits each), as in the previous example.

6.1.3 Comments on the test results

We stress that the above presented good results are typical, even if changing the parameter γ to a different small value, provided to satisfy (30). We have tried at random dozens of PRNGs with $n = 32, 64$ and $b = 3, 4, 5, 6, 7, 8$, with different values of γ, obtaining similar results. If $b = 4$ (or 8) we output the 2 (or 3) most significant bits of $\tilde{x}$ at each time step. For the other values, we set an under-sampling rate equal to $p = 8$, whereas outputting the most significant byte (8 bits). As a general trend, it seems that for the kind of generators proposed in this paper the most sensitive test is the Non Overlapping Template. The focus of this test, according to the default parameters, is the number of occurrences of 148 different non-periodic patterns of 9-bits. In some cases it happened that the passing rate for some patterns dropped to 96.0% when analyzing 100 sequences of 2 million bits each (the theoretical requested minimum passing rate is 96.0150%). Nevertheless, apart from this minor and occasional statistical imperfection, in all of the evaluated PRNGs none of the tests in the NIST SP800.22 standard were badly failed (the worst PRNG found had a 94.0% passing rate in one test).

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

generator is <N64K2P1_4.000000000001838A_2Mb_100Seq.dat>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	6	15	14	13	14	9	14	5	3	0.032923	0.9900	Frequency
11	14	10	7	5	13	10	14	10	6	0.419021	0.9800	BlockFrequency
11	6	6	14	13	10	14	11	5	10	0.350485	0.9900	CumulativeSums
8	9	8	6	14	13	15	7	10	10	0.494392	0.9800	CumulativeSums
8	8	14	8	7	8	9	16	12	10	0.514124	1.0000	Runs
9	7	13	11	8	7	8	14	11	12	0.759756	1.0000	LongestRun
4	10	11	16	13	11	11	10	6	8	0.319084	1.0000	Rank
7	6	16	9	11	14	7	11	13	6	0.249284	0.9900	FFT
									mean:	0.459514	0.9916	NonOverlTemplate (*)
								standard deviation:		0.292429	0.0095	
8	9	10	7	15	7	12	12	10	10	0.779188	0.9900	OverlappingTemplate
9	8	11	10	5	16	15	15	5	6	0.071177	0.9800	Universal
10	13	11	10	9	9	7	10	9	12	0.978072	0.9900	ApproximateEntropy
									mean:	0.441598	0.9911	RandomExcursions (*)
								standard deviation:		0.278924	0.0106	
									mean:	0.612595	0.9960	RandomExcVariant (*)
								standard deviation:		0.225489	0.0082	
8	8	14	10	7	13	8	11	8	13	0.739918	1.0000	Serial
12	10	13	12	10	7	5	8	12	11	0.739918	0.9800	Serial
11	11	8	8	11	6	18	7	12	8	0.289667	0.9900	LinearComplexity

(*) Test with multiple results: mean value and standard deviation were reported.

Table 1: NIST800.22 test results for the PRNG based on $\tilde{T} = \tilde{S}_\beta$, with $n = 64$ bits and $\beta =$ `0x4.000000000001838A`. At each time step the 2 most significant bits of $\tilde{x}$ were output.

7 Conclusions

In this work we have proposed the design of PRNGs based on nonlinear recurrences derived from the Rényi chaotic map. Starting from a weaker interpretation of the Shadowing Theory proposed by Coomes et al. we have theoretically framed the relationship that exists between the Rényi chaotic maps and their digitized versions. Exploiting the ergodic properties of the original systems we have proposed a method for the design of nonlinear recurrences whose statistical behavior can be analyzed in terms of chaotic dynamics approximation. In order to overcome the problem of the shortness in the period length of the digitized trajectories, we have proposed to perturb the pseudo-chaotic dynamics in such a way to emulate the orbit instability peculiar to chaotic systems. Statistical tests confirm the validity of the approach, that is general and define an infinite family of PRNGs that can be used to approximate the statistical behavior of an ideal TRNG with an arbitrary accuracy.

Appendix

Proof of Theorem 2

We first need the following

Lemma 2 *Let $\frac{q_0}{2^n} \in \Lambda_n$ and $z > \frac{q_0}{2^n}$. If the restriction of the Rényi map S_β to the interval $J = \left[\frac{q_0}{2^n}, z\right)$ is continuous, for any $x \in J$ and for any $m \in \mathbb{N}$, with*

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

generator is <N32K8P8_7.000000AA0_2Mb_100Seq.dat>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
7	10	10	7	10	14	10	6	15	11	0.574903	0.9900	Frequency
10	11	9	10	8	9	12	10	8	13	0.983453	1.0000	BlockFrequency
8	6	14	10	10	8	10	15	5	14	0.304126	1.0000	CumulativeSums
8	11	6	11	8	11	8	12	9	16	0.616305	0.9900	CumulativeSums
15	9	8	5	17	7	12	10	11	6	0.145326	1.0000	Runs
15	12	11	9	9	7	9	13	9	6	0.657933	0.9800	LongestRun
9	10	15	8	8	9	8	3	18	12	0.075719	0.9800	Rank
14	7	7	13	10	10	10	5	17	7	0.181557	0.9900	FFT
									mean:	0.495993	0.9895	NonOverlTemplate (*)
								standard deviation:		0.295015	0.0094	
10	16	13	8	9	8	16	7	9	4	0.137282	0.9700	OverlappingTemplate
12	10	11	13	9	13	9	12	9	2	0.401199	0.9900	Universal
9	8	9	9	10	10	11	17	8	9	0.719747	0.9700	ApproximateEntropy
									mean:	0.368254	0.9896	RandomExcursions (*)
								standard deviation:		0.281558	0.0126	
									mean:	0.368254	0.9896	RandomExcVariant (*)
								standard deviation:		0.281559	0.0126	
11	11	11	12	10	12	6	4	12	11	0.657933	0.9900	Serial
11	11	14	7	10	9	6	12	11	9	0.834308	1.0000	Serial
8	14	7	9	10	10	12	14	11	5	0.574903	1.0000	LinearComplexity

(*) Test with multiple results: mean value and standard deviation were reported.

Table 2: NIST800.22 test results for the PRNG based on $\tilde{T} = \tilde{S}^8_\beta$, with $n = 32$ bits and $\beta =$ `0x7.000000AA0`. Every eight iterations of $\tilde{S}^8_\beta$ the 8 most significant bits of $\tilde{x}$ were output.

$q_0 \leq m \leq \lfloor 2^n z \rfloor$, *it results*

$$\left| S_\beta(x) - \tilde{S}_b\left(\frac{m}{2^n}\right)\right| < \beta \left| x - \frac{m}{2^n}\right| + \frac{1}{2^n}.$$

Proof. We note that if S_β is continuous over J, then it has a constant slope: for any $x_1, x_2 \in J$ we have $|S_\beta(x_2) - S_\beta(x_1)| = \beta|x_2 - x_1|$. Moreover, we note that for any $\frac{m}{2^n} \in \Lambda_n$ it results $\left|S_\beta\left(\frac{m}{2^n}\right) - \tilde{S}_\beta\left(\frac{m}{2^n}\right)\right| < \frac{1}{2^n}$, indeed

$$\begin{aligned} \tilde{S}_\beta\left(\frac{m}{2^n}\right) = \frac{\lfloor \beta m \bmod 2^n \rfloor}{2^n} \leq \frac{\beta m \bmod 2^n}{2^n} = S_\beta\left(\frac{m}{2^n}\right) < \\ < \frac{\lfloor \beta m \bmod 2^n \rfloor + 1}{2^n} = \tilde{S}_\beta\left(\frac{m}{2^n}\right) + \frac{1}{2^n}. \end{aligned} \tag{46}$$

Accordingly,

$$\begin{aligned} \left|S_\beta(x) - \tilde{S}_\beta\left(\frac{m}{2^n}\right)\right| = \left|S_\beta(x) - S_\beta\left(\frac{m}{2^n}\right) + S_\beta\left(\frac{m}{2^n}\right) - \tilde{S}_\beta\left(\frac{m}{2^n}\right)\right| \leq \\ \leq \left|S_\beta(x) - S_\beta\left(\frac{m}{2^n}\right)\right| + \left|S_\beta\left(\frac{m}{2^n}\right) - \tilde{S}_\beta\left(\frac{m}{2^n}\right)\right| < \beta\left|x - \frac{m}{2^n}\right| + \frac{1}{2^n}, \end{aligned}$$

concluding the proof. □

We can now prove the main Theorem.

Proof of Theorem 2. We will prove the theorem focusing on the inequality

$$\left|S^p_b(x) - \tilde{S}^p_\beta(\tilde{x})\right| \leq \left|S^p_b(x) - S^p_\beta(x)\right| + \left|S^p_\beta(x) - \tilde{S}^p_\beta(\tilde{x})\right|, \tag{47}$$

and noting that $K_2 \subset K_1$. Let us assume the Rényi map continuous on intervals containing the points $S_\beta^j(x)$ and $\tilde{S}_\beta^j(\tilde{x})$, for $j = 0, 1, \ldots, p-1$. From the Lemma 2 we have

$$\left|S_\beta^{j+1}(x) - \tilde{S}_\beta^{j+1}(\tilde{x})\right| < \beta \left|S_\beta^j(x) - \tilde{S}_\beta^j(\tilde{x})\right| + \frac{1}{2^n},$$

and proceeding by induction it is easy to prove that

$$\left|S_\beta^j(x) - \tilde{S}_\beta^j(\tilde{x})\right| < \beta^j|x - \tilde{x}| + \frac{1}{2^n}\sum_{r=0}^{j-1}\beta^r = \beta^j|x - \tilde{x}| + \frac{\beta^j - 1}{(\beta - 1)\cdot 2^n}. \tag{48}$$

Due to the truncation strategy (29) we have $|\tilde{x} - x| < 1/2^n$, and the previous inequality becomes

$$\left|S_\beta^j(x) - \tilde{S}_\beta^j(\tilde{x})\right| < \frac{\beta^{j+1} - 1}{(\beta - 1)2^n}. \tag{49}$$

Since $K_2 \subset K_1$ we can use the result (32), and by setting $j = p$ the ineq. (47) is verified. The proof is completed if we show that if $x \in S_b^{-p}(K_2)$ then some intervals exist containing the points $S_\beta^j(x)$ and $\tilde{S}_\beta^j(\tilde{x})$, for $j = 0, 1, \ldots, p-1$, and in which the Rényi map is continuous (this allows the use of the previous Lemma).

Accordingly, we define the set $P_\beta = \{\frac{i}{\beta}, 0 < i \leq b\}$ and we note that for $j = 0$ the previous condition is satisfied if the distance of x from the nearest point in P_β is not smaller than $\frac{1}{2^n}$: this is a sufficient condition to avoid a discontinuity point of S_β lying between x and $\tilde{x}$. For the second step, since we know from (49) that $|S_\beta(x) - S_b(x)| < \frac{\beta+1}{2^n}$, a sufficient condition to have both of the points $S_\beta(x), \tilde{S}_\beta(\tilde{x})$ in a same interval between two discontinuity points of S_β is to have $S_\beta(x)$ not closer than $\frac{1}{2^n} + \frac{\beta+1}{2^n}$ to the nearest point in P_β. Generalizing, for $j = 0, \ldots, p-1$ both of the points $S_\beta^j(x), S_b^j(x)$ lye in a same interval between two discontinuity points of S_β if $S_\beta^j(x)$ is not closer than

$$\frac{1}{2^n}\left(1 + \sum_{r=0}^{j} b^r\right) = \frac{\beta^{j+1} + \beta - 2}{(\beta - 1)2^n} \tag{50}$$

to the nearest point in P_β.

By using the result (32), the above condition is verified if $S_b^j(x)$ is not closer than

$$\frac{\beta^{j+1} + \beta - 2}{(\beta - 1)2^n} + \left(1 - \frac{b}{\beta}\right)\frac{b^{j+1} - b}{b - 1} \tag{51}$$

to the nearest point in P_β. Again, the latter condition is verified if $S_b^j(x)$ is not closer than

$$\begin{aligned}\left(1 - \frac{b}{\beta}\right) + \frac{\beta^{j+1} + \beta - 2}{(\beta - 1)2^n} + \left(1 - \frac{b}{\beta}\right)\frac{b^{j+1} - b}{b - 1} = \\ = \frac{\beta^{j+1} + \beta - 2}{(\beta - 1)2^n} + \left(1 - \frac{b}{\beta}\right)\frac{b^{j+1} - 1}{b - 1}\end{aligned} \tag{52}$$

to the nearest point in P_b.

Let us now focus on the set K_2: we will show that for $m = 1, \ldots, p$ the set $S_b^{-m}(K_2)$ contains only points that satisfy the previous sufficient conditions.

In detail, we note that the set $S_b^{-1}(K_2)$ is made of b intervals of the form $[\frac{i}{b}+\frac{\delta_2}{b}, \frac{i}{b}+\frac{1-\delta_2}{b})$ for $0 \leq i < b$, that is, each point in $S_b^{-1}(K_2)$ is not closer than $\frac{\delta_2}{b}$ to the nearest point in P_b. Following the same reasoning, it is easy to check that each point in $S_b^{-m}(K_2)$ is not closer than $\frac{\delta_2}{b^m}$ to the nearest point in P_b. Accordingly, in order to satisfy the previously discussed sufficient conditions, it suffices that

$$\frac{\delta_2}{b^{p-j}} \geq \frac{\beta^{j+1}+\beta-2}{(\beta-1)2^n} + \left(1-\frac{b}{\beta}\right)\frac{b^{j+1}-1}{b-1}, \tag{53}$$

that is

$$\delta_2 \geq b^{p-j}\frac{\beta^{j+1}+\beta-2}{(\beta-1)2^n} + \left(1-\frac{b}{\beta}\right)\frac{b^{p+1}-b^{p-j}}{b-1}. \tag{54}$$

On the other hand for $j = 0, \ldots, p-1$,

$$\frac{b^{p+1}-b^{p-j}}{b-1} < \frac{b^{p+1}-b}{b-1}, \tag{55}$$

and

$$b^{p-j}\frac{\beta^{j+1}+\beta-2}{(\beta-1)2^n} \leq \beta^{p-j}\frac{\beta^{j+1}+\beta}{(\beta-1)2^n} = \frac{\beta^{p+1}\left(1+\beta^{-j}\right)}{(\beta-1)2^n} < \frac{2\beta^{p+1}}{(\beta-1)2^n}. \tag{56}$$

As a result, if $\delta_2 = \frac{2\beta^{p+1}}{(\beta-1)2^n} + \left(1+\frac{b}{\beta}\right)\frac{b^{p+1}-b}{b-1}$ the inequality (54) is verified and the proof is completed. □

References

[1] A. Menezes, P. Van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997.

[2] C. Petrie and A. Connelly, "A noise-based IC random number generator for applications in cryptography," *IEEE Transaction on Circuits and Systems I*, vol. 47, no. 5, pp. 615–621, 2000.

[3] T. Addabbo, M. Alioto, A. Fort, S. Rocchi, and V. Vignoli, "A variability-tolerant feedback technique for throughput maximization of TRBGs with predefined entropy," *Journal of Circuits, Systems and Computers*, vol. 19, no. 4, pp. 1–17, 2010.

[4] ——, "A feedback strategy to improve the entropy of a chaos-based random bit generator," *IEEE Transaction on Circuits and Systems – part I*, vol. 53, no. 2, pp. 326–337, 2006.

[5] S. Callegari, R. Rovatti, and G. Setti, "Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos," *IEEE Trans. on Signal Processing*, vol. 53, no. 2, pp. 793–805, 2005.

[6] M. Bucci, L. Germani, R. Luzzi, P. Tommasino, A. Trifiletti, and M. Varanonuovo, "A high-speed IC random-number source for smartcard microcontrollers," *IEEE Transaction Circuits and Systems I*, vol. 50, no. 11, pp. 1373–1380, 2003.

[7] P. Walters, *An Introduction to Ergodic Theory*. Springer, 1982.

[8] J. Boyar, "Inferring sequences produced by pseudo-random number generators," *Journal of the ACM*, vol. 36, no. 1, pp. 129–141, 1989.

[9] J. B. Plumstead, "Inferring a sequence produced by a linear congruence," in *CRYPTO*, 1982, pp. 317–319.

[10] D. Knuth, *The art of computer programming*, 2nd ed. Addison-Wesley, 1981, vol. 2.

[11] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, 1986.

[12] "NIST Special Publication 800-22 Rev.1a: A statistical test suite for random and pseudorandom number generators for cryptographic applications," Apr. 2010.

[13] B. Coomes, H. Kocak, and K. Palmer, *Six Lectures on Dynamical Systems*. World Scientific, 1996, ch. Shadowing in Discrete Dynamical Systems, pp. 163–211.

[14] J. Eichenauer-Herrmann, "Pseudorandom number generation by nonlinear methods," *International Statistical Reviews*, vol. 63, pp. 247–255, 1995.

[15] S. Tezuka, *Uniform Random Numbers: Theory and Practice*. Kluwer Academic Publishers, 1995.

[16] J. Eichenauer-Herrmann, "Inversive congruential pseudorandom numbers avoid the planes," *Mathematics of Computation*, vol. 56, pp. 297–301, 1991.

[17] S. W. Golomb, *Shift Register Sequences*. Laguna Hills, CA: Aegean Park, 1982.

[18] J. Eichenauer and A. Topuzŏglu, "On the period length of congruential pseudorandom number sequences generated by inversions," *Journal of Computational and Applied Mathematics*, vol. 31, pp. 87–96, 1990.

[19] W. A. Beyer, R. B. Roof, and D. Williamson, "The lattice structure of multiplicative congruential pseudo-random vectors," *Mathematics of Computation*, vol. 25, no. 114, pp. 345–363, 1971.

[20] A. Boyarsky and P. Góra, *Laws of Chaos*. Birkhäuser, 1997.

[21] T. Addabbo, A. Fort, S. Rocchi, D. Papini, and V. Vignoli, "Invariant measures of tunable chaotic sources: Robustness analysis and efficient computation," *IEEE Transactions on Circuits and Systems - I*, vol. 56, no. 4, pp. 806–819, 2009.

[22] T. Addabbo, A. Fort, D. Papini, S. Rocchi, and V. Vignoli, "An efficient and accurate method for the estimation of entropy and other dynamical invariants for piecewise affine choatic maps," *International Journal of Bifurcation and Chaos*, vol. 19, no. 12, pp. 4175 – 4195, 2009, accepted.

[23] G. Setti, G. Mazzini, R. Rovatti, and S. Callegari, "Statistical modeling of discrete-time chaotic processes: basic finite-dimensional tools and applications," *Proc. of the IEEE*, vol. 90, no. 5, pp. 662–690, 2002.

[24] T. Stojanovski and L. Kocarev, "Chaos-based random number generator – part I: Analysis," *IEEE Transactions on Circuits and Systems I*, vol. 48, no. 3, pp. 281–288, 2001.

[25] A. Lasota and M. C. Mackey, *Chaos, Fractals and Noise - Stochastic Aspects of Dynamics*, 2nd ed. Springer, 1994.

[26] J. Amigó, L. Kocarev, and I. Tomovski, "Discrete entropy," *Physica D*, vol. 228, pp. 77–85, 2007.

[27] L. Kocarev and A. J. Szczepanski, "Discrete chaos–I: Theory," *IEEE Transaction on Circuits and Systems – I*, vol. 53, no. 6, pp. 1300–1309, June 2006.

[28] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, and V. Vignoli, "A class of maximum-period nonlinear congruential generators derived from the Rényi chaotic map," *IEEE Transactions on Circuits and Systems - I*, vol. 54, no. 4, pp. 816–828, 2007.

[29] T. Addabbo, A. Fort, L. Kocarev, S. Rocchi, and V. Vignoli, "Pseudo-chaotic lossy compressors for true random number generation," *IEEE Transaction on Circuits and Systems I*, 2010, submitted.

[30] T. Addabbo, D. De Caro, A. Fort, N. Petra, S. Rocchi, and V. Vignoli, "Efficient implementation of pseudochaotic piecewise linear maps with high digitization accuracies," *International Journal of Circuit Theory and Applications*, 2010.

[31] R. Devaney, *An Introduction to Chaotic Dynamical System*, 2nd ed. Addison-Wesley, 1989.

[32] F. Pareschi, G. Setti, and R. Rovatti, "Noise robustness condition for chaotic maps with piecewise constant invariant density," in *ISAS 2004*, vol. IV, 2004, pp. 681–684.