Commun Nonlinear Sci Numer Simulat 43 (2017) 139–150

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

journal homepage: www.elsevier.com/locate/cnsns

Research paper

Measuring the jitter of ring oscillators by means of information theory quantifiers

M. Antonelli[a], L. De Micco[a,b,*], H.A. Larrondo[a,b]

[a] ICYTE (Instituto de Investigaciones Científicas y Tecnológicas en Electrónica) Facultad de Ingeniería, Universidad Nacional de Mar del Plata Juan B. Justo 4302, Mar del Plata Buenos Aires, Argentina
[b] CONICET (Consejo Nacional de Investigaciones Científicas y Técnicas), Argentina

ARTICLE INFO

Article history:
Received 24 February 2016
Accepted 2 May 2016
Available online 6 May 2016

Keywords:
Entropy
FPGA
Jitter
Ring oscillators

ABSTRACT

Ring oscillators (*RO*'s) are elementary blocks widely used in digital design. Jitter is unavoidable in *RO*'s, its presence is an undesired behavior in many applications, as clock generators. On the contrary, jitter may be used as the noise source in *RO*-based true-random numbers generators (*TRNG*). Consequently, jitter measure is a relevant issue to characterize a *RO*, and it is the subject of this paper. The main contribution is the use of Information Theory Quantifiers (*ITQ*) as measures of *RO*'s jitter. It is shown that among several *ITQ* evaluated, two of them emerge as good measures because they are independent of parameters used for their statistical determination. They turned out to be robust and may be implemented experimentally. We encountered that a dual entropy plane allows a visual comparison of results.

1. Introduction

Jitter is any light deviation from the mean period of a presumed periodic signal. There are many physical examples where jitter is relevant. Some examples from different areas are: (a) Stalberg et al [1] found that the time interval between the two fibre action potentials of two muscle fibers -belonging to the same motor unit in the normal human muscles- shows a variability or jitter; (b) Mecozzi et al [2] detected timing and amplitude jitter in optical links using highly dispersed pulse transmission; (c) Derickson et al [3] made a comprehensive timing jitter comparison in the case of mode-locked semiconductor lasers; (d) the California and Carnegie Planet Search at Keck Observatory [4] reported jitter in stars radial velocities; (e) Roberts & Guillemin studied the delays due to queueing in upstream multiplexing stages, in an Asynchronous Transfer Mode network (ATM); (f) Baron et al [5] considered the quality of the bunch clock signal of the Large Hadron Collider (LHC), in terms of jitter, a fundamental issue because it synchronizes all the electronics systems in the detector; (g) Marsalek et al analyzed the relationship between synaptic input and spike output jitter in individual neurons [6], etc.

Furthermore, digital instruments are used in any modern experiment and the unavoidable jitter in the data acquisition systems produces uncertainties in time, and consequently in any spectrum determination.

This paper is devoted to Ring Oscillators (*RO*). Let us stress that in this particular application jitter is not always undesirable. Jitter is unwanted in applications that use the *RO* as a clock generator [7–11]. On the contrary random numbers

* Corresponding author. Tel.: +54223155635283; fax: +542234869900.
E-mail addresses: ldemicco@fi.mdp.edu.ar (L. De Micco), larrondo@fi.mdp.edu.ar (H.A. Larrondo).

http://dx.doi.org/10.1016/j.cnsns.2016.05.002
1007-5704/

generators *RNG* using *RO*'s, use jitter as the randomness source, [12,13]. Jitter also improves the Electromagnetic Compatibility as to distribute the clock frequency over a band, improving the Electromagnetic Compatibility (EMC) [14].

Determination of jitter in *RO*'s has been studied in several papers: in [15] the study of three relevant time domain measures of jitter was presented. In [16] a model for jitter generation and distribution in *RO*'s was proposed. In this seminal paper the authors brake up the jitter sources into deterministic and random (gaussian); furthermore each source is additionally classified into local or global. They demonstrate that the most important contributions are the local gaussian jitter and the global deterministic jitter and only the first one must be used as a randomness source of true random number generators (*TRNG*'s). The same approach was used in [17–20]. Lubicz et al. described a practical and efficient method to estimate the entropy rate of a *TRNG* based on free running oscillators; they emphasized that their method does not require outputting and analyzing the clock signals with external equipment [21] (a methodology that introduces extra jitter and distortion in the measured signal due to the data acquisition chain).

Usually *deterministic jitter* is the name given to any *non-Gaussian jitter*. It is bounded and it is characterized by its peak to peak Δ_{pp} value. Random jitter is the name used for Gaussian jitter and it is unbounded and characterized by its RMS value. Sometimes deterministic periodic jitter appears. It has a *period* that is the interval between two times of maximum (minimum) effect; the inverse of the time period is *the frequency of the jitter*. Periodic jitter with jitter frequency below 10*Hz* is usually named *wander* and the name *jitter* is reserved only to periodic jitter with frequencies at or above 10*Hz*. In communications, the *total jitter* is $T = \Delta_{pp} + 2\,n\,R_{rms}$ where n is a number between 6 and 8 related to the Bit Error Rate (*BER*).

RO's are one of the main building blocks in analog and digital integrated circuits and have been extensively used as *on-chip oscillators* to generate clocks in high-speed circuits. Furthermore, *RO*'s can be easily implemented in programmable digital circuits like *FPGA*'s. The main advantages of *RO*'s over integrated *LC* oscillators are their smaller chip area, their wider running range (that may be electrically tuned), and their lower power-consumption.

Either one wants to use the *RO* jitter or to eliminate it, jitter must be measured, and it is not a simple task. The main contribution of this paper is to provide a jitter measurement technique based on information theory quantifiers (*ITQ*). We use a stochastic model which randomness is related to the jitter strength. Every proposed *ITQ* used in this paper is based on an entropy, that is a Shannon functional of the probability distribution function (*PDF*) assigned to the time series of the stochastic process. Disequilibrium and complexities may be used as well [22,23] but they do not represent an improvement in our case. In previous works [24,25] we showed that many different *PDF*'s can be assigned to the same data string. The best choice depends on the specific application. Two choices for the *PDF* are used in this paper: the *normalized histogram* and the *ordering patterns histogram*. A representation plane is used to compare different situations. Once a *PDF* is chosen, the Shannon Entropy is the basic functional that quantifies the uniformity of the *PDF*. *Normalized entropies*, *differential entropies*, and *rate entropies* are the other *ITQ*'s evaluated. In our case *differential entropies* give the best results and a *differential entropy plane* is used to compare their sensitivity as a jitter measure.

Organization of the paper is as follows: Section 2 describes jitter in *RO*'s and explains how it is measured using random variables; Section 3 details the evaluation of the considered *ITQ*; Section 4 deals with the results using the proposed quantifiers. Finally, we present our conclusions in Section 5.

2. Determination of jitter in *RO*'s

There are two different situations concerning jitter in *RO*'s: (a) for some applications it is enough to assure that jitter does not perturb the signal over an accepted limit. If this is the case the signal is observed on an oscilloscope with a mask over the display and it is enough to verify that the signal remains within tolerances; (b) in other cases an exact determination of jitter is required. One of these cases is the characterization of *RO*'s, considered in this paper.

Ideal *RO*'s are composed of an odd number of inverters. Each inverter has a propagation time and consequently rising and falling edges separated by half-periods go through the inverters. If all the propagation times are constant the output of this *ideal RO* is a square-wave with a discrete spectrum. But propagation times are not constant as there is jitter. Jitter distorts the delta like power spectrum as each δ is converted into a wider maximum.

Let $T/2$ be the half-period of the *ideal RO*. It is given by:

$$\frac{T}{2} = k\sum_{i=1}^{k} d_i \tag{1}$$

where k is the number of inverters and d_i is the propagation time through the $i-$th inverter. When jitter exists, d_i are random variables that can be modeled as:

$$d_i = D_i + \Delta d_i \tag{2}$$

where D_i is the mean value of d_i with nominal source voltage level and normal temperature, and $\triangle d_i$ is the delay variation produced by both local physical events and global changes in the device working conditions (as VCC, temperature, etc.). Then jitter in *RO*'s is evidenced by the random displacement of the trailing (falling) edges from their otherwise perfectly periodic location. The direct measurement of this displacement has two main problems: (a) requires a very high-frequency instrument, because time resolution is limited by the sampling period T_s; (b) this technique introduces extra jitter and distortions

in the measured signal coming from the data acquisition chain. Then it is more convenient to use *indirect measurements*, by means of auxiliary random variables related to statistical properties related with jitter to measure jitter with minimal disturbance [21]. The general procedure is as follow:

1. Sample the output with sampling period T_s to get a binary time series. In the ideal case of *no-jitter* the output is a *continuous and perfectly periodic square wave* with period T. Then it is possible to adjust T_s to make $T/2 = m\,T_s$ with $m \in N^+$. The binary time series will be periodic with m *1*'s followed by m *0*'s. When jitter is present the binary series is not periodic but stochastic. This stochastic model is known as *alternating renewal process*.
2. Many different randomness quantifiers may be used to characterize the stochastic model associated with the measured jitter. In this paper, we propose the use of *ITQ*'s.

Note that jitter is accumulative and two basic situations arise: (a) if the jitter introduced by each stage is assumed to be totally independent of the jitter introduced by other stages, it means $\sigma_T^2 = m * \sigma_s^2$, where σ_s is the jitter of each sample, and it is supposed that all samples have jitter with the same normal distribution; (b) if jitter sources are totally correlated with one another then $\sigma_T = m * \sigma_s$.

3. Information theory quantifiers

3.1. Time series and probability distribution functions

Shannon Entropy is the functional of P more frequently used in the literature (there are other functionals, like statistical complexity, disequilibrium, etc.). An important issue is P itself is not a uniquely defined object and do exist several approaches to "associate" a given P with a given time series. Just to mention some extraction procedures frequently used in the literature: *(a)* time series histogram [26], *(b)* binary symbolic-dynamics [27], *(c)* Fourier analysis [28], *(d)* wavelet transform [29,30], *(e)* partition *PDF* [31], *(f)* permutation *PDF* [32,33], *(g)* discrete *PDF* [34], etc. There is ample liberty to choose among them and the specific application must be analyzed to make a good choice.

The general procedure to assign P to a given time series consists in the following steps:

- (a) define an alphabet $\mathfrak{A} = \{s_j, j = 1, \ldots m\}$
- (b) convert the time series $X = \{x_i, i = 1, \ldots\}$ into a *symbolic sequence* $A = \{a_i, a_i \in \mathfrak{A}\}$.
- (c) P is given by the relative frequencies of the symbols: $P = \{p_j, j = 1, \ldots, m\}$ in the symbolic sequence A, where p_j is the relative frequency of symbol s_j.

P may be *non-causal* or *causal* [24] depending on step b. P is *non-causal* when one symbol $s_j \in \mathfrak{A}$ is assigned to each value $x_i \in X$. For example, the usual histogram technique used for time series of real numbers corresponds to this kind of assignment. Of course, in this method the temporal order of the time-series plays no role, and consequently the resulting P will not have any *causal information* and the *symbolic sequence* may be simply regarded as a *coarse-grained* description of X [24]. It is also possible to group W consecutive values of the time series -a *trajectory* of length W- and assign one symbol to the group. Note that this procedure is equivalent to first assign a symbol to each value of the time series, then group W symbols into a *word* and finally construct a new alphabet consisting of words. If the original alphabet has m elements, there will be m^W possible words and one of this words will be assigned to the *trajectory* of W elements. P is given by the relative frequencies of all the possible words. Here P depends on the temporal order of X and consequently we call it a *causal P*. It is interesting to note that a *causal P* has information about statistics and also about temporal ordering of X. If a *non-causal P* is used instead, the analysis must be complemented with the evaluation of the Fourier transform, or the autocorrelation function of X, to recover the information about temporal ordering.

Let us stress even more the difference between a *non-causal* and a *causal P* by means of the following simple example. Let $X = \{x_i, i = 1, 2, \ldots\}$ be a time series generated by *randn* (Matlab's© function); let $Y = \{y_i, i = 1, 2, \ldots\}$ be the resulting series after a sorting process made by *sort* (Matlab's© function). Fig. 1(a) and 1(b) show the time series. One noncausal P is the normalized histogram, and $P(X)$ is identical to $P(Y)$ as Fig. 1(c) and 1(d) reveal. One causal P may be obtained by the Bandt & Pompe procedure (for details about its determination see below) and Fig. 1(e) and 1(f) show that $P(X)$ and $P(Y)$ are completely different: $P(X)$ is almost uniform, reflecting X is randomly ordered, but $P(Y)$ has a delta-like shape, as far as Y is monotone increasing and only one ordering pattern is present.

Let us consider now the case of sampled digital signals like as sampled *RO*'s outputs are. Time series X is binary and has a natural alphabet with two symbols $\mathfrak{A} = \{0, 1\}$. The Shannon entropy of this alphabet is usually known as *Binary Entropy* S_2. Suppose W consecutive bits of X are grouped into *a word*, that is the decimal number w_i between 0 and $2^W - 1$; consider these decimal numbers as the symbols of the new alphabet and let $Z = \{w_i, i = 1, 2, \ldots\}$ be the new symbolic series. S_W is the entropy of $P_{hist}(Z)$ where subscript *hist* is for histogram; S_W is also known as *Block Entropy* of the binary time series X. Furthermore, if D consecutive decimal numbers w_i are grouped again and the $D!$ permutation patterns are considered as symbols of the new alphabet, we get a new $P_{BP}(Z)$, given by the relative frequencies of the permutation patterns. The entropy is $S_{BP}^{(D)}$, the *Bandt & Pompe entropy* [32] of the binary time series. All the above-mentioned entropies are given by

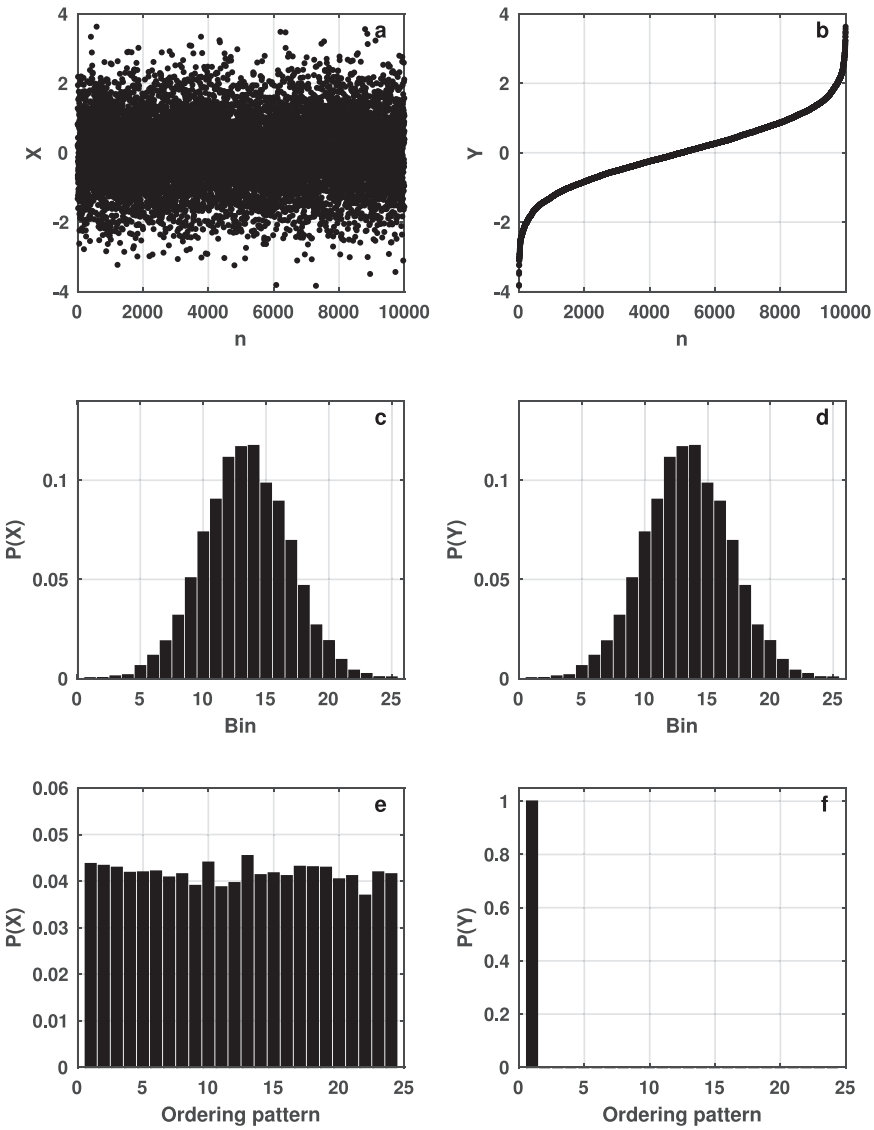

Fig. 1. (see text) Time series X obtained by using function *randn* (a), its sorted version Y (b) and their causal (c, d) and normalized (e, f).

the same Shannon famous formula:

$$S = -\sum_{j=1}^{m} p_j \log(p_j), \tag{3}$$

and the only difference between them is the P assigned to the time series. In this paper *log* means *base* 2 *logarithm*.

In this paper, we use a causal P determined with the Bandt & Pompe procedure. This procedure has been described in detail and successfully used in a number of papers concerning true random number generation, system classifications, etc. [22–25,35,36]. Let us summarize the basic procedure applied to our specific case:

- let $Z = \{w_i,\ i = 1, 2, \ldots\}$ be a numerical time series (in our case W bits decimal numbers) series;
- choose an embedding dimension $D > 1$
- assign to each w_i a D-dimensional vector of previous $i, i-1, \cdots, i-(D-1)$:

$$(s) \mapsto \left(w_{i-(D-1)}, w_{i-(D-2)}, \cdots, w_{i-1}, w_i\right) \tag{4}$$

  Clearly, the greater the D−value, the more information about "the past" is incorporated into these vectors.
- look for *ordinal patterns* of length D [32,33,37]. By "ordinal pattern" related to position i we mean the permutation $\pi = (r_0, r_1, \cdots, r_{D-1})$ of $(0, 1, \cdots, D-1)$ defined by

$$w_{i-r_{D-1}} \le w_{i-r_{D-2}} \le \cdots \le w_{i-r_1} \le a_{i-r_0} \tag{5}$$

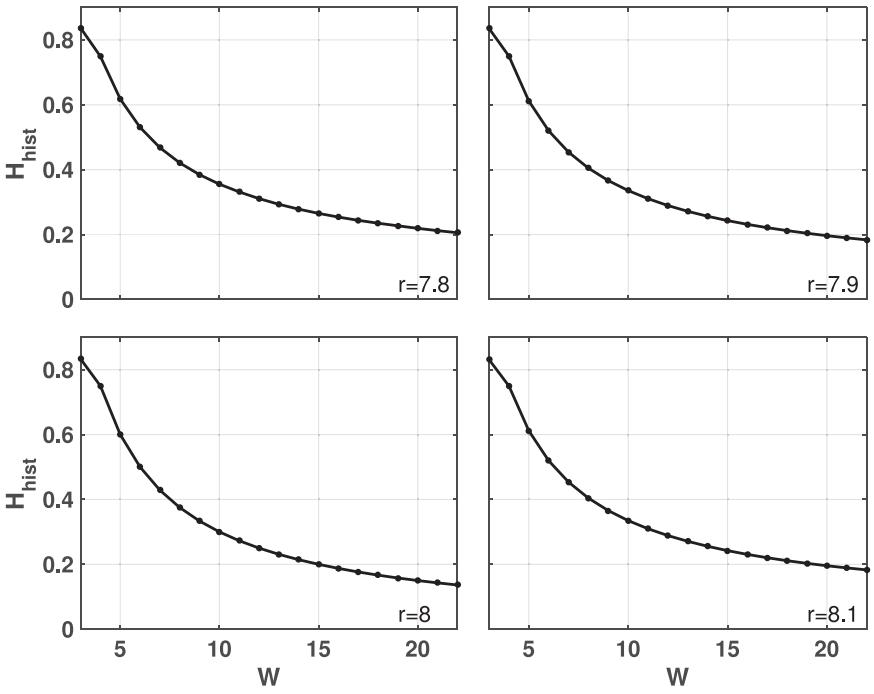

Fig. 2. Normalized entropy H_W as a function of W for a jitter-less RO sampled with different values of r.

- In order to get a unique result consider that $r_j < r_{j-1}$ if $x_{i-r_j} = x_{i-r_{j-1}}$.
- Thus for all the $D!$ possible permutations π of order D is the probability distribution $P = \{p(\pi)\}$ defined by

$$p(\pi) = \frac{\sharp\{s | s \leq M - D + 1; i \quad \texttt{has type}\, \pi\}}{M - D + 1} \tag{6}$$

In the last expression, the symbol $\sharp$ stands for "number" and corresponds to the number assigned to the permutation using the lexicographic order .

The main advantages of the Bandt & Pompe method are *(a)* its simplicity, *(b)* the extremely fast nature of the pertinent calculation-process, *(c)* its robustness in the presence of observational and dynamical noise, and *(d)* its invariance with respect to nonlinear monotonous transformations. The Bandt & Pompe methodology is not restricted to time series representative of low dimensional dynamical systems but can be applied to any type of time series (regular, chaotic, noisy, or reality based), with a very weak stationary assumption (for $k = D$, the probability for $a_i < a_{i+k}$ should not depend on i [32]).

Let us stress some important issues involved in the calculations of the above-mentioned entropies:

1. The binary entropy S_2 is noncasual while both, the block entropy S_W and the Bandt and Pompe entropy $S_{BP}^{(D)}$, are causal.
2. The block entropy S_W takes into account correlations between W consecutive bits. Bandt & Pompe entropy $S_{BP}^{(D)}$ takes into account correlations between D consecutive W-length words. Both grouping procedures (decimal numbers of W bits and permutation patterns of D decimal numbers) may be done with or without superposition. The number of data required for good statistics is different depending the grouping procedures are made with superposition or not.
3. For S_W there is only one grouping process (W bits are grouped to obtain a decimal numbers time series Y). Let us define α as a statistical quality parameter, given by the quotient between the number of elements in the symbolic time series Y and the number of symbols in the alphabet. In this paper we will not accept $\alpha < 10$.
   Obviously the quality factor α increases with the length of the time series:
   (a) If the grouping of W bits is made with superposition, two consecutive W-length words share $W - 2$ bits. Consequently starting with a file with a length of N-bits we get $N - W + 1$ words. Furthermore, there are 2^W symbols in the alphabet and $\alpha = (N - W + 1)/(2^W)$.
   (b) If S_W is evaluated without superposition the number of W-length words is $floor\ \{N/W\}$ and the quality parameter becomes $\alpha = floor\{N/W\}/(2^W)$. For $N \gg W$ the statistical quality factor is W times lower that the one with superposition.
4. In the case of $S_{BP}^{(D)}$, there are two grouping processes involved.

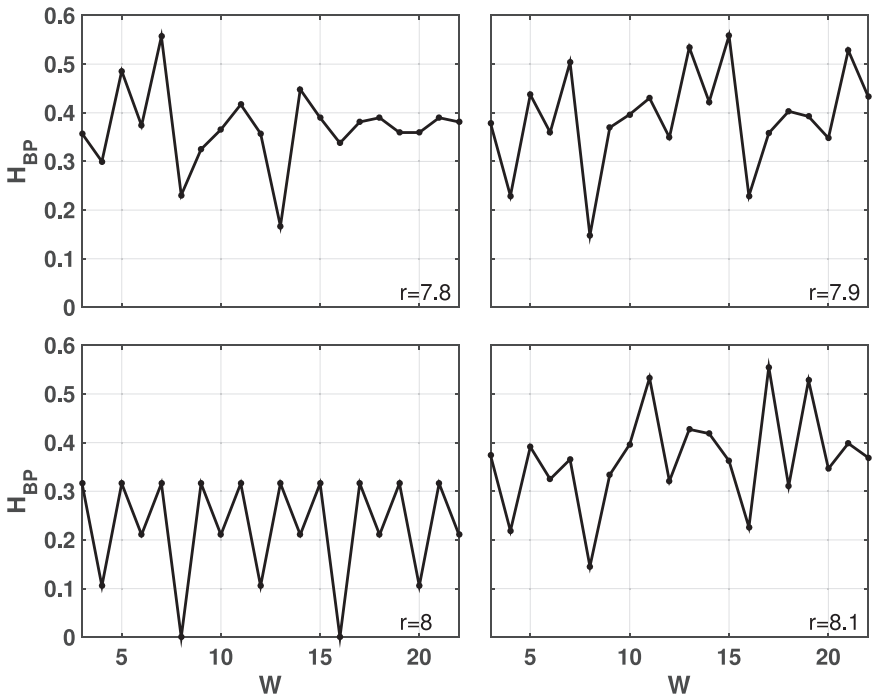

Fig. 3. $H_{BP}^{(D)}$ as a function of W for a jitter-less *RO* sampled with different values of r. Calculations are made without superposition of words.

(a) If both grouping processes are made with superposition we get $N-W-D+2$ elements starting with a file N-bits length, and the quality factor is $\alpha = (N-W-D+2)/D!$. In this case $S_{BP}^{(D)}$ takes into account the correlations between $W+D$ consecutive bits.
(b) If the grouping process of W bits is made without superposition but the grouping of D decimal numbers is made with superposition we get $floor\{N/W\}-D+1$ elements and the statistical quality parameter is $\alpha = (floor\{N/W\}-D+1)/D!$. In this case $S_{BP}^{(D)}$ will include correlations between WD consecutive bits.
(c) If the grouping process of W bits is made with superposition and the grouping of D decimal numbers is made without superposition we get $floor\{(N-W+1)/D\}$ elements starting from a file with N bits.The statistical quality factor is $\alpha = floor\{(N-W+1)/D\}/D!$ and $S_{BP}^{(D)}$ takes into account correlations between $W+D-1$ bits.
(d) If both grouping processes are made without superposition we get $floor\{floor\{N/W\}/D\}$ elements starting from a N-bits length file. The statistical quality factor is $\alpha = floor\{floor\{N/W\}/D\}/D!$ and $S_{BP}^{(D)}$ takes into account correlations between WD consecutive bits.

3.2. Additional quantifiers

The Shannon Entropy $S(P)$ is the startpoint for other quantifiers:

1. Normalized entropy $H(P)$: it is the Shannon Entropy divided by its maximum value. For example, if we use S_2 (see above), the maximum entropy is obtained for equiprobability between two symbols. Its value is $S_{max} = -1/2log(1/2) - 1/2log(1/2) = log(2) = 1$; then, the normalized entropy is $H_2 = S_2$. If we use S_W the equiprobability between the 2^W possible words (W-bits decimal numbers) produces $S_{max} = W$ and $H_W = S_W/W$. Finally for $S_{BP}^{(D)}$ the equiprobability between the $D!$ ordinal patterns produces $S_{max} = log(D!)$ and $H_{BP}^{(D)} = S_{BP}^{D}/log(D!)$.
2. Differential or conditional entropies h and h^* are:

$$h = S_{W+1} - S_W \tag{7}$$

$$h^* = S_{BP}^{(D+1)} - S_{BP}^{(D)} \tag{8}$$

In the above expressions $W = 1, 2, \ldots$ and $D = 2, 3, \ldots$, $S_0 = 0$ and $S_{BP}^{(1)} = 0$. These differential or conditional entropies give the average amount of information required to predict the $(W+1)$ (or $(D+1)$) symbol, given the preceding W (or D) symbols.
3. Finally the *rate entropies* h_0 and h_0^* are given by:

$$h_0 = \lim_{W\to\infty} h = \lim_{W\to\infty} S_W/W \tag{9}$$

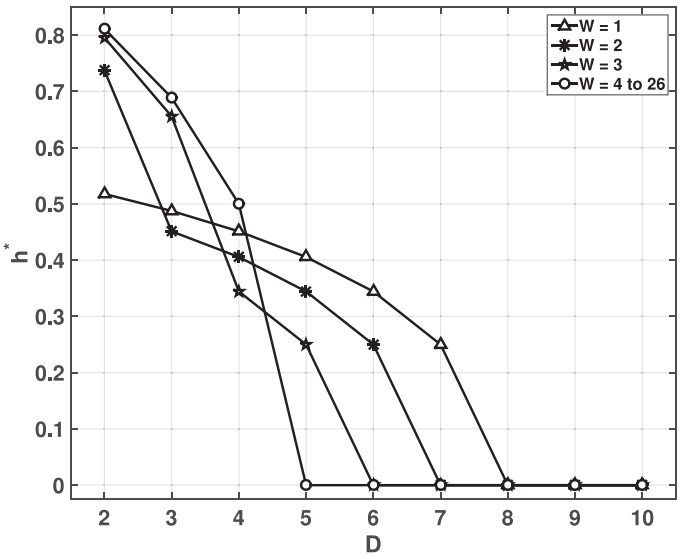

Fig. 4. h^* as a function of D for a jitter-less *RO* sampled with $r = 8$.

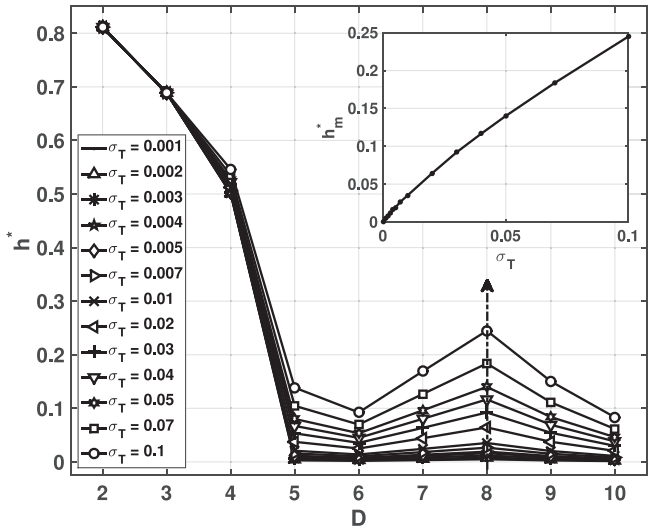

Fig. 5. h^* as a function of D for a *RO* sampled with $r = 8$ for a world length $W = 6$ for jitter with several variances. The inset shows h^* as a function of σ_T for $r = 8$, $W = 6$ and $D = 8$.

$$h_0^* = \lim_{D\to\infty} h^* = \lim_{D\to\infty} S_{BP}^{(D)}/(D-1) \tag{10}$$

Let us tell in advance that we shall show in Section 4 that quantifiers S_W, $S_{BP}^{(D)}$, H_W and $H_{BP}^{(D)}$ are dependent on parameters W and D. This is a drawback if we want to use them as jitter measures. On the other hand, the estimators h and h^* of the *rate entropies* h_0 and h_0^* [22,31] instead, are independent of W and D and we will show in Section 4 that in the case of sampled *RO*'s they also present a minimum for the correct sampling ratio making them good measure of the quality of both *RO*'s and *TRNG*'s derived from them.

4. Results

An evenly sampled output of a jitter-less *RO* was simulated with Matlab© and an output file with a length of $N_b = 7,000,000$ of bits was generated. A set of a hundred values of the sampling ratio $r = T_s/T \in [6.5, 9.5]$, was explored (where T_s is the sampling period and T is the *RO* output period). Jitter with a normal distribution and a set with different values of variance σ_s (see below) were added to the original file. Our method emulates the real process of sampling the noisy output of a real *RO*; the detailed code is published in Mathworks [38].

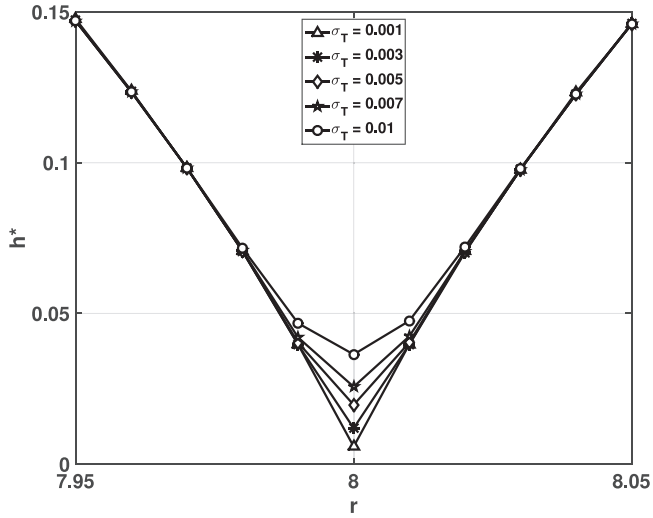

Fig. 6. h^* as a function of r for $r \in [7.95, 8.05]$, with several σ_T, $W = 6$ and $D = 8$. The curve has a minimum at the correct value $r = 8$.

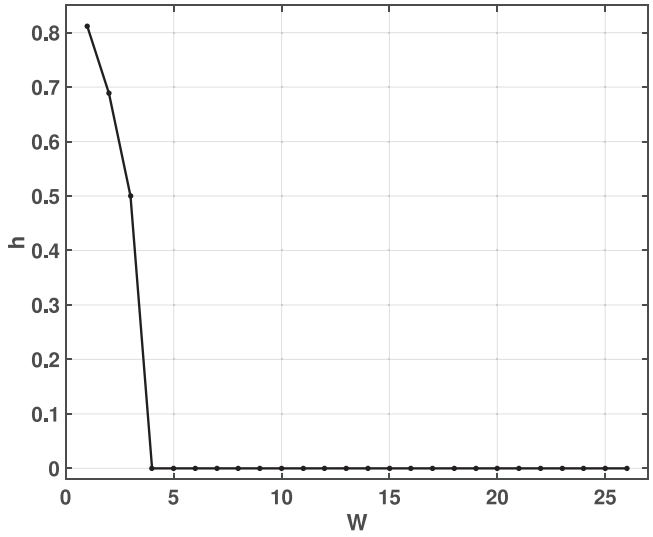

Fig. 7. h as a function of W for a jitter-less *RO* sampled with $r = 8$.

For each value of σ_s, ten surrogates (each one with a different random initial condition) were generated and new files with N_b bits each were stored. It was assumed that jitter of individual samples is independent, normal distributed random variables, with zero mean value and variance $\sigma_i = \sigma_s$. Consequently, the variance of the accumulated jitter over one period T is given by $\sigma_T^2 = r\sigma_s^2$ [16]. The values considered are $\sigma_T = \{0,\ 0.001,\ 0.002,\ 0.003,\ 0.004,\ 0.005,\ 0.007,\ 0.01,\ 0.02,\ 0.02,\ 0.04,\ 0.05,\ 0.07,\ 0.1\}$.

For each file all the quantifiers defined in Section 3 were evaluated for $D \in [2, 10]$ and $W \in [1, 26]$. The details about evaluation, advantages and drawbacks of each quantifier are reported in Section 3: they are S_W, $S_{BP}^{(D)}$, H_W, $H_{BP}^{(D)}$, h and h^*. Let us only show here the more relevant results to show the reason the last two quantifiers (h and h^*) are the best ones.

- In the case of normalized entropy H_W, it strongly depends on W. Furthermore the analysis of H_W as a function of r shows that it does not allow to determine an optimum value of the sampling ratio r (see Fig. 2). This is an important issue if the quantifiers are going to be used for experimental setups.
- In the case of the normalized Bandt & Pompe entropy $H_{BP}^{(D)}$, a strong dependence on the embedding dimension D is additionally present. Again it is not easy to determine the optimum value of r from the analysis of this parameter as a function of r (see Fig. 3).
- A similar behavior appears in all the other functionals related with these two entropies. In summary, our results show that both h y h^* are independent of any arbitrary parameter used in their statistical determination. These two quantifiers have also been considered in two excellent articles [31,39].

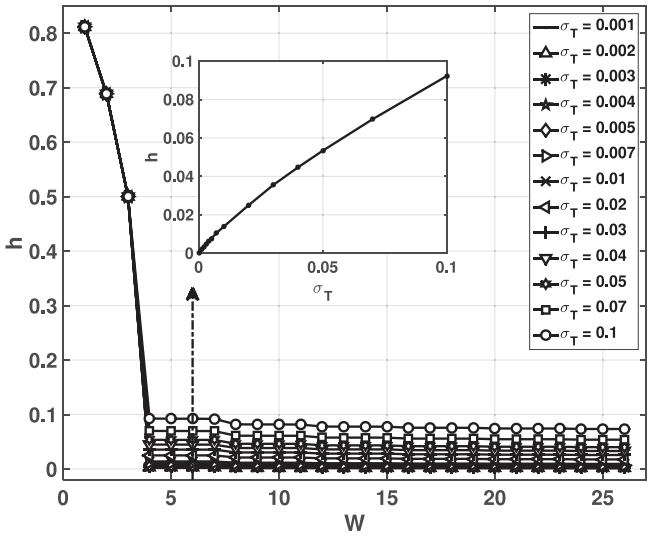

Fig. 8. h as a function of W for a *RO* sampled with $r = 8$, for jitter with several variances. The inset shows h as a function of σ_T for $r = 8$ and $W = 6$.

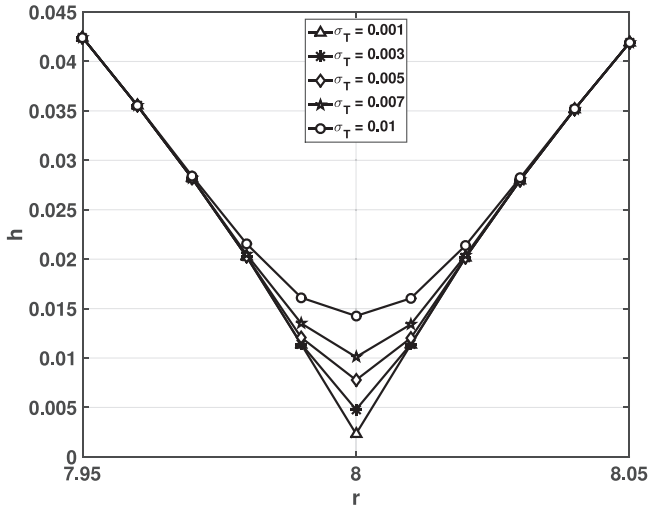

Fig. 9. h as a function of r for $r \in [7.95, 8.05]$, with several σ_T and $W = 6$. The curve has a minimum at the optimum value $r = 8$.

Our results show that two quantifiers, h and h^*, are appropriate to be used as jitter measures because:

- (a) for $\sigma_T = 0$ (jitter-less output) they rapidly approach to a constant limiting value as both D and W increase toward ∞ and this limiting value is independent of both D and W;
- (b) they are increasing monotone (and almost proportional) functions of σ_T.
- (c) From their analysis, it is possible to detect the optimum value of the sampling ratio r. Let us show these claims in the following figures that are representative of all our results.

Fig. 4 shows the Bandt & Pompe differential entropy h^*, as a function of D, with W as a parameter, for a ring without jitter. It can be seen that there is a threshold value $W = 4$ over which all the curves collapse into one for every value of D. Furthermore, Fig. 4 also shows that for $D \geq 8$ all the curves collapse into one, regardless the value of W. In conclusion, if $D \geq 8$ and $W \geq 4$ one obtains a quantifier independent of both D and W. The influence of jitter on this quantifier is shown in Fig. 5, where h^* is plotted as a function of D with σ_T as a parameter. The values considered are $\sigma_T = \{0(no\ jitter),\ 0.001,\ 0.002,\ 0.003,\ 0.004,\ 0.005,\ 0.007,\ 0.01,\ 0.02,\ 0.02,\ 0.04,\ 0.05,\ 0.07,\ 0.1\}$. The inset of Fig. 5 shows h^* as a function of σ_T for $D = 8$. This inset shows that this quantifier is an increasing monotone function of σ_T. Finally Fig. 6 shows h^* as a function of the sampling ratio r. In this figure, it is shown that there is a minimum for the right r (in this case $r = 8$). Furthermore sensitivity of h^* as a function of jitter is maximum for this same ideal value of r.

Let us now analyze the second quantifier, h. This quantifier only depends on W because D is not used to define the *PDF* assigned to the data series. Fig. 7 shows jitter-less case, h is almost independent of W for $W \geq 4$. In this paper, we adopted

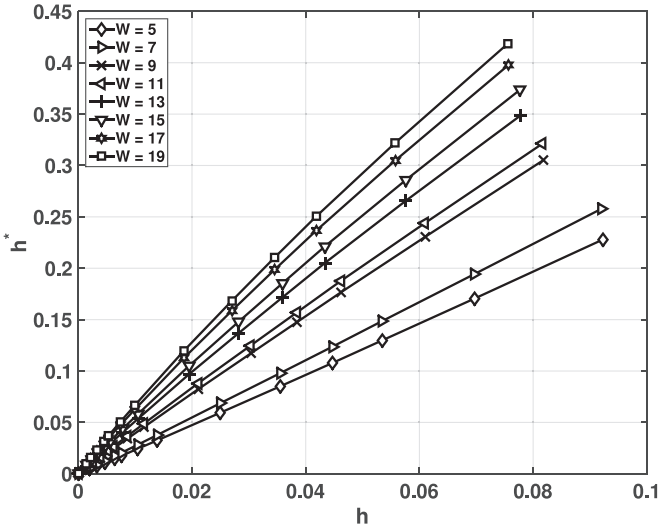

Fig. 10. h^* as a function of h for $r = 8$, $D = 8$ and different values of W.

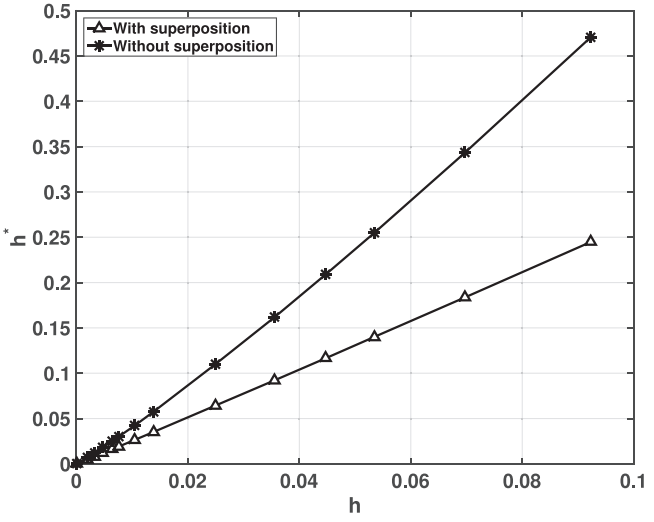

Fig. 11. h^* as a function of h for $r = 8$, $W = 6$ and $D = 8$. Two procedures to obtain W-bits natural numbers are considered: with and without superposition (see text).

$W = 6$. Fig. 8 shows the influence of jitter over this quantifier. It is clear from the inset in this figure that, for the selected value $W = 6$, h is an increasing monotone function of jitter variance σ_T.

Fig. 9 shows that h has a minimum when the value of r takes its optimum value ($r = 8$). Note that this minimum is robust also in the presence of jitter.

Further analysis must be done to assure that the selected values $W = 6$ and $D = 8$ produce symbolic files with a good statistics. For a given alphabet $\mathcal{A}$ with m elements, and a given symbolic file of length n, the quality parameter $\alpha = n/m$, see Section 3. Quality is better as α increases and a minimum value $\alpha = 10$ was accepted. According to Section 3 the selected values $W = 6$ and $D = 8$ provide $\alpha_h \simeq 10^5$, $\alpha_{h^*} \simeq 175$ with superposition and 29 without superposition. All cases give $\alpha > 10$ as required.

A comparison between both quantifiers is shown in Fig. 10. Markers correspond to variances $\sigma_T = \{0, 0.001, 0.002, 0.003, 0.004, 0.005, 0.007, 0.01, 0.02, 0.03, 0.04, 0.05, 0.07, 0.1\}$. Note that the slope of any of these curves is dh^*/dh and it is equal to the quotient between slopes of curves in the insets of Figs. 5 and 8. If $dh^*/dh > 1$, h^* is more sensitive than h to measure jitter. The slope slightly increases from ~ 2.47 for $W = 5$ to ~ 5.54 for $W = 19$ showing that h^* becomes more sensitive as W increases.

We also evaluated h^* without the superposition of bits between consecutive natural numbers but keeping the superposition of $D - 1$ natural numbers between ordering patterns (In all cases h was evaluated with superposition of $W - 1$ consecutive bits). Results are depicted in Fig. 11 where it is shown that removing the superposition the sensitivity of this

quantifier increases. Of course, we get a smaller amount of W bits natural numbers form the original seven million binary file, and consequently, the statistical quality is lower than that of the original calculation with superposition. To increase α up to its previous value, longer binary files are required.

5. Conclusions

Given their usefulness as *TRNG* and clock generators, *RO*s are becoming one of the main building blocks of digital circuits. Jitter is unavoidable in *RO*'s, and consequently, it needs to be characterized. Mixing and distribution of values are the main properties to consider. Several *ITQ* quantifiers were evaluated here. S_W, $S_{BP}^{(D)}$, H_W and $H_{BP}^{(D)}$ turn out to be dependent on parameters W and D. This is a drawback if we use them as jitter measures. On the other hand, it is no possible to calculate *rate entropies*, h_0^* and h_0, since an infinite number of data is necessary for their calculation. The two *differential entropies*, h^* and h, instead, are independent of the parameters used for their determination and are estimators of the *rate entropies*. We have shown in Section 4 that in the case of sampled *RO*s they also present a minimum for the correct sampling ratio making them a good measure of the quality of both *RO*'s and *TRNG*'s derived from them.

The dual entropy plane determined by these quantifiers has demonstrated to satisfactorily discern between the *TRNG*'s two main desired properties, the equiprobability among all possible values and the statistical independence between consecutive values. Thus, it allows clearly seeing what needs to be improved in a given sequence. The examples presented here have demonstrated the need to use both histograms for characterizing sequences.

Acknowledgment

This work was partially supported by the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET)(PIP 112-200801-01420), ANPCyT (PICT-2013-2066), International Centre for Theoretical Physics (ICTP) Associateship Scheme and UNMDP Argentina.

References

[1] Beomsup K, Helman DN, Gray PR. The electromyographic jitter in normal human muscles. Electroencephal Clinical Neurophysiol 1971;31:429–38.
[2] Mecozzi A, Clausen CB, Park S-G, Gnauck AH. Cancellation of timing and amplitude jitter in symmetric links using highly dispersed pulses. IEEE Photonics Technol Lett 2001;13(5):445–7.
[3] Derickson DJ, Morton PA, Bowers JE, Thornton RL. Comparison of timing jitter in external and monolithic cavity mode-locked semiconductor lasers. Appl Phys Lett 1991;59:3372–4. doi:10.1063/1.105704.
[4] Wright JT. Radial velocity jitter in stars from the california and carnegie planet search at keck observatory. Publications Astron Society Pacific 2005;117:657–64.
[5] Baron S, Mastoridis T, Troska J, Baudrenghien P. Jitter impact on clock distribution in lhc experiments. Topical Workshop on Electronics for Particle Physics 2012. IOP for SISSA Media Lab; 2012. doi:10.1088/1748-0221/7/12/C12023.
[6] Marsalek CK, MAUNSELL J. On the relationship between synaptic input and spike output jitter in individual neurons. Neurobiology 1997;94:735–40.
[7] Javier SL-B, Garrido J, Boemo E. Thermal testing on programmable logic devices. IEEE Intl Symp Circuits Syst 1998;2:240–3.
[8] Beomsup K, Helman DN, Gray PR. A 30-mhz hybrid analog/digital clock recovery circuit in 2-?m cmos.. J Solid-State Circuits 1990;25(6):1385–94.
[9] Hajimiri A, Limotyrakis S, Lee TH. Jitter and phase noise in ring oscillators. IEEE J Solid-State Circuits 1999.
[10] Mandal MK, Sarkar BC. Ring oscillators: Characteristics and applications. Indian J Pure Appl Phys 2010;48:136–45.
[11] Gupta N. Article: Voltage-controlled ring oscillator for low phase noise application. Int J Comput Appl 2011;14(5):23–7. Published by Foundation of Computer Science.
[12] Sunar B, Martin WJ, Stinson DR. A provably secure true random number generator with built-in tolerance to active attacks. IEEE Trans Comput 2007;56(1):109–19. http://doi.ieeecomputersociety.org/10.1109/TC.2007.4.
[13] Wold K, Tan CH. Analysis and enhancement of random number generator in fpga based on oscillator rings. Int J Reconfig Comput 2009;2009. 4:1–4:8
[14] De Micco L, Petrocelli RA, Rosso OA, Plastino A, Larrondo HA. Mixing chaotic maps and electromagnetic interference reduction. Intl J Appl Math Statis 2012;26:106–20.
[15] McNeill JA. Jitter in ring oscillators. IEEE J Solid State Circuits 1997;32(6):870–9.
[16] Valtchanov B, Aubert A, Bernard F, Fischer V. Modeling and observing the jitter in ring oscillators implemented in fpgas. In: Straube B, Drutarovsk M, Renovell M, Gramata P, Fischerov M, editors. DDECS. IEEE Computer Society; 2008. p. 158–63. ISBN 978-1-4244-2276-0.
[17] Fischer V, Bernard F, Bochard N, Varchola M. Enhancing security of ring oscillator-based trng implemented in fpga. In: FPL; 2008. p. 245–50.
[18] Valtchanov B, Fischer V, Aubert A, Bernard F. Characterization of randomness sources in ring oscillator-based true random number generators in fpgas. In: Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2010 IEEE 13th International Symposium on; 2010. p. 48–53.
[19] Baudet M, Lubicz D, Micolod J, Tassiaux A. On the security of oscillator-based random number generators.. J Cryptol 2011;24(2):398–425.
[20] Jessa M, Matuszewski L. Enhancing the randomness of a combined true random number generator based on the ring oscillator sampling method. In: Reconfigurable Computing and FPGAs (ReConFig), International Conference on; 2011. p. 274–9.
[21] Lubicz D, Bochard N. Towards an oscillator based trng with a certified entropy rate. Comput IEEE Trans 2014;PP(99). doi:10.1109/TC.2014.2308423. 1–1
[22] Amigó JM, Kennel B, Kocarev L. The permutations entropy rate equals the metric entropy rate for ergodic information sources and ergodic dynamical systems. Physica D 2005;210:77–95. http://dx.doi.org/10.1016/j.physd.2005.07.006.
[23] Rosso OA, Zunino L, Pérez DG, Figliola A, Larrondo HA, Garavaglia M, et al. Extracting features of gaussian selfsimilar stochastic processes via the bandt & pompe approach. Phys Rev E 2007;76(6):061114.
[24] De Micco L, González CM, Larrondo HA, Martin MT, Plastino A, Rosso OA. Randomizing nonlinear maps via symbolic dynamics. Physica A 2008;387:3373–83.
[25] De Micco L, Larrondo HA, Plastino A, Rosso OA. Quantifiers for randomness of chaotic pseudo random number generators. Philosophical Trans Royal Society A 2009;367:3281–96.
[26] Martin MT. Ph.d. thesis, department of mathematics,. Faculty of Sciences, University of La Plata; 2004.
[27] Mischaikow K, Mrozek M, Reiss J, Szymczak A. Construction of symbolic dynamics from experimental time series. Phys Rev Lett 1999;82:1114–47.
[28] Powell GE, Percival IC. A spectral entropy method for distinguishing regular and irregular motion of hamiltonian systems. J Phys A: Math Gen 1979;12:2053–71.
[29] Blanco S, Figliola A, Quian Quiroga R, Rosso OA, Serrano E. Time-frequency analysis of electroencephalogram series (iii): Wavelet packets and information cost function. Phys Rev E 1998;57:932–40.

[30] Rosso OA, Blanco S, Jordanova J, Kolev V, Figliola A, Schürmann M, et al. Wavelet entropy: a new tool for analysis of short duration brain electrical signals. J Neuroscience Meth 2001;105:65–75.
[31] Ebeling W, Steuer R. Partition-based entropies of deterministic and stochastic maps. Stochastics Dyn 2001;1(1):1–17.
[32] Bandt C, Pompe B. Permutation entropy: a natural complexity measure for time series. Phys Rev Lett 2002;88. 174102–1
[33] Keller K, Sinn M. Ordinal analysis of time series. Physica A 2005;356:114–20.
[34] Amigó JM, Kocarev L, Tomovski I. Discrete entropy. Physica D 2007;228:77–85.
[35] Amigó JM. Permutation complexity in dynamical systems. Springer-Verlag, Berlin, Germany; 2010.
[36] Rosso OA, Vicente R, Mirasso C. Encryption test of pseudo-aleatory messages embedded on chaotic laser signals: an information theory approach. Phys Lett A 2008;372:1018–23.
[37] Keller K, Lauffer H. Symbolic analysis of high-dimensional time series. Int J Bifurcation and Chaos 2003;13:2657–68.
[38] Antonelli M.. Emulating a ring oscillator with jitter. www.mathworks.com/matlabcentral/fileexchange/54021-jitter-samples-n-r-sigma-; 2015.
[39] Amigó JM, Kocarev L, Szczepanski J. Order patterns and chaos. Phys Lett A 2006;355:27–31.