Noise and chaos contributions in fast random bit sequence generated from broadband optoelectronic entropy sources

Xiaole Fang, Benjamin Wetzel, Jean-Marc Merolla, John M. Dudley,
Laurent Larger, Christophe Guyeux, Jacques M. Bahi University of Franche-Comté
FEMTO-ST institute, UMR CNRS 6174, Besançon, France
Email: laurent.larger@univ-fcomte.fr

***Abstract*—During the last 4 years, chaotic waveforms for random number generation found a deep interest within the community of analogue broadband chaotic optical systems. Earlier investigations on chaos-based RNG were proposed in the 90s and early 2000, however mainly based on piecewise linear (PL) 1D map, with bit rate determined by analog electronic processing capabilities to provide the PL nonlinear function of concern. Optical chaos came with promises for much higher bit rate, and entropy sources based on high complexity (high dimensional) continuous time (differential) dynamics. More specifically in 2009, Reidler *et al.* published a paper entitled "An optical ultrafast random bit generator", in which they presented a physical system for a random number generator based on a chaotic semiconductor laser. This generator is claimed to reach potentially the extremely high rate of 300 Gb/s. We report on analysis and experiments of their method, which leads to the discussion about the actual origin of the obtained randomness. Through standard signal theory arguments, we show that the actual binary randomness quality obtained from this method, can be interpreted as a complex mixing operated on the initial analogue entropy source. Our analysis suggests an explaination about the already reported issue that this method does not necessarily require any specific deterministic property (i.e. chaos) from the physical signal used as the physical source of entropy. The bit stream randomness quality is found to result from "aliasing" phenomena performed by the post-processing method, both for the sampling and the quantization operations. As an illustration, such random bit sequences extracted from different entropy sources are investigated. Optoelectronic noise is used as a non deterministic entropy source. Electro-optic phase chaotic signal, as well as simulations of its deterministic model, are used as deterministic entropy sources. In all cases, the extracted bit sequence reveals excellent randomness.**

***Keywords*-Random number generation, chaos, optoelectronics, noise, entropy sources, statistical tests**

I. Introduction

Random Number Generators (RNGs) are widely used in science and technology. They are a critical component in modern cryptographic systems, communication systems, statistical simulation systems, and any scientific area incorporating Monte Carlo methods and many others [1]–[3]. The unpredictability of the bit stream and the speed at which the random bits can be produced are usually reported as very important aspects in the quality of the generated bit sequence. Other factors like system complexity, cost, reliability and so on, are also important for establishing successful RNGs. There are usually two methods for RNGs: One relates to deterministic algorithms implemented in hardware and software, the pseudorandom numbers being generated from a single "seed" (such generators are named pseudorandom number generators, or PRNGs in short); Another one counts on high entropy signals, whether from mainly nondeterministic and stochastic physical phenomena (see [4]–[7]), or from deterministic but chaotic dynamical systems [7]–[11]. A potential advantage of the latter physical high entropy signal, arises in its deterministic features that might be used to achieve chaos synchronization as it has been already demonstrated [12] and widely used for secure optical chaos communications [13]. However, synchronization possibility of the random binary sequence extracted from the chaotic physical signal is still an open problem, which resolution could lead to the efficient and practical use of the one-time pad (a symmetric encryption algorithm derived from the Vernam cipher, which is proven to be impossible to crack if used under appropriate conditions).

The PRNGs based on deterministic algorithms can be implemented in any computational platform, some can even be easily adapted with discrete chaotic iterations to improve output quality of randomness [14]. They however suffer from the vulnerability that the future sequence can be deterministically computed if the seed or internal state of the algorithm is discovered. The main advantage of PRNGs is that no hardware cost is added, and the speed is only counted on digital processing hardware. Their algorithms are developed to prevent guessing of the initial conditions, and the rate might be slowed down while increasing the complexity of such algorithms.

Physical RNGs rely on chaotic or stochastic physical processes. Such random number generators are building the random bits from inherently random or chaotic physical process [15], for example, radioactive decay [16], chaotic electrical and optical circuits [17], and so on. Up to recently, the implementations of physical random generators have been limited to much slower rates than PRNGs because of limitation of the mechanisms for extracting bits from physical randomness without degrading statistical properties. Typically 10 Mb/s could be achieved by using electronic oscillator jitter [18] and 4 Mb/s using quantum optical noise [19]. One should notice however, that such physical implementation was recently directly developed at the chip level in personal computer processors, finally achieving more than reasonable speed performances ($>$ 3 Gb/s), and actually also very good randomness quality [20].

Considerable improvements for the rate of chaotic random bits generation have been however reached by using a semi-

conductor laser in the presence of external feedback [21], a well known setup in chaotic optical systems. The dynamical processes involved in optical systems can indeed be very fast. Moreover, high complexity chaotic dynamics can be practically obtained, whether due to intrinsic complex nonlinear coupling between light and matter interactions in lasers, or due to the presence of a large delay feedback cavity enabling dynamics with large number of degrees of freedom.

Chaotic optical signal might consist of pulses with a width of few 10ps and with random amplitude and time positions, which provide attractive potentials to easily generate random bits at fast rates. In [9], a first attempt already reached 1.7 Gb/s RNG, the physical randomness originating from two independent chaotic semiconduct lasers. Each laser intensity signal is practically sampled at an incommensurate rate with respect to the individual optical feedback delay times. Then a threshold value is set for comparison with each signal level and to obtain a Boolean sequence. Lastly the random bit sequence is produced by executing a XOR function between the two Boolean sequences. More recently, Reidler and colleagues [22], [23] claim that they successfully demonstrated another method in generating random bit sequence from ultra fast optical chaos, at much faster rate. In such method, the output of a single chaotic laser, with the optical feedback delay time incommensurate with the sampling clock frequency, was digitized by an 8-bit analog-to-digital converter (ADC, practically provided by an ultra-fast digital scope). Then the difference between adjacent, but not nearest, points from the 8-bit digitized time series is performed (it is defined as a pseudo-"derivative" operation). At last, a few LSBs only of the values resulting from the subtracted samples are retained to generate the binary sequence. Following this combination of broadband photonic chaos and digital post-processing, generation rate as high as 300 Gb/s are claimed. Many additional papers have then appeared [24]–[30], utilizing similar bit stream extraction method, but on different alternative photonic setups. These reported works have claimed to have achieved comparable high speed and high randomness quality bit stream. None of these papers has however discussed the actual and respective roles played by the photonic chaotic waveform on one side, and by the post-processing method on the other side.

In this paper, the study of using broadband optical signal to generate random binary sequence according to the method proposed by Reidler, is going to be deepen. We propose to apply the same method on the chaotic waveform generated by another class of broadband photonic oscillations, and to analyze the different post-processing steps involved in this method. We will analyze three key factors in the scheme of [22] and [23]: the sampling, the difference of distant samples, and LSBs retaining.

The paper is organized in the following way. In Section II, the original architecture that we propose as the physical system to generate fast random bit sequences, is described in details. Analysis of the conversion of the physical time series into a binary random sequence as proposed in [23] is recalled, but also analyzed in terms of signal processing arguments. Then an entropy evaluation for the binary sequence is processed in Section III, thus providing insight for the entropy rate capability for the generated binary sequence. Finally, the randomness quality of the obtained bit sequence is compared, depending on the used physical signal: whether a chaotic laser intensity, or a noisy signal covering a similar Fourier spectrum. The randomness quality is evaluated in Section IV via the results of four statistical testing packages. The paper ends with a discussion of the obtained results, and concludes with possible future work.

II. Method for Random Bit Sequence Generation from an Optoelectronic Signal

In this section we describe the physical setup from which we expect to obtain a fast random bit sequence. We also describe the binary sequence extraction method from the continuous time signal generated by the physical setup, as it was formerly proposed in [22], [23]. Additionally, theoretical interpretations and discussions of this extraction method are proposed in terms of basic signal processing and sampling theory. These interpretation and discussion are intended to give insight on the possible mechanisms at the origin of the bit stream randomness quality.

A. Setup delivering a broadband optoelectronic signal

In order to additionally support our work with experiments on the generation of optical broadband signals, data recorded from physical chaos generator as well as from optoelectronic noise sources, have been studied. These experiments are different from the ones described in [22] and [23], although they are also originating from broadband optoelectronic devices.

A twofold physical source of entropy has been used (see Fig.1), both having been tested for their randomness quality. One source (referred as "Optoelectronic noise" in Fig.1) is originating from physical noise sources in the semiconductor laser light generation process (known as RIN: relative intensity noise), in combination with the electronic noise of the photodetector and its integrated electronic amplifier (thermal noise and semiconductor photodiode junction noise, amplified by the noise figure of the electronic amplifier). A comparable (and even cheaper) optoelectronic noise source was also proposed in [5], [31].

On the contrary, the other physical source of entropy is originating from a strongly deterministic process, which was used for a field experiment demonstrating (analogue) chaotic optical masking of 10 Gb/s data signals, transmitted over an installed fiber optic link [32]. The strong determinism of this entropy source indeed enabled to implement accurate broadband chaos synchronization at the receiver, in order to remove the chaotic masking signal and thus to retrieve the original binary data stream. The dynamics of the electro-optical phase chaos generator is ruled by a nonlinear dual delay differential equation implemented in an optoelectronic and electro-optic feedback loop.

Each of these two signals obtained from noise or chaotic optoelectronic systems, has been processed by using the method proposed in [22]. By doing so, the aim is to support our signal processing analysis on the extraction method of the bit sequence, which is inferring that in both cases, the randomness quality must be very similar. As we shall illustrate and discuss later, and as it has been pointed only in the literature [4], chaos is not a necessary condition for a good randomness quality of the extracted bit stream. Global spectral and statistical features in the original analogue source of entropy appear to be

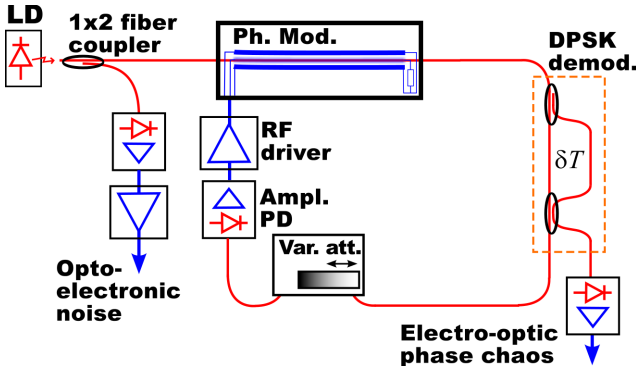


Fig. 1: Experimental setup of the optical system used to generate signal as physical random sources for the derivation of random bit sequences.

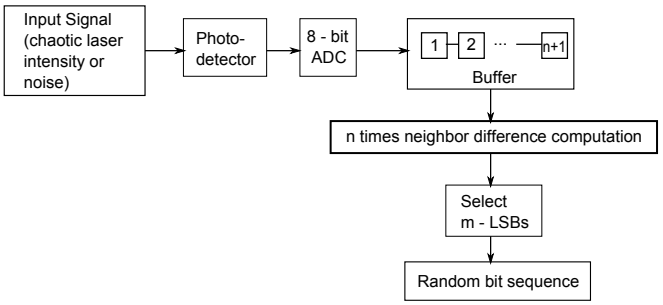


Fig. 2: Scheme of the RNG using optical signal

enough, such as a broadband Fourier spectrum, and a sufficient spreading of the amplitude probability distribution.

Instead of using necessarily noise corrupted signal as it is always the case in experiments, one can also generate time traces numerically, thus resulting in an even stronger determinism in the entropy source. In that case, the noise level is significantly reduced to numerical rounding and numerical integration errors. One however needs a suitable deterministic model in order to generate such numerical time traces. Our deterministic chaotic signal is modeled by the physical solution of a nonlinear dual delay dynamics ruled by the following differential equation:

$$\theta^{-1}\int_0^t x(\xi)d\xi + \tau\frac{dx}{dt}(t) + x(t) = \beta\sin^2[x_T - x_{T+\delta T} + \Phi_0], \tag{1}$$

where x_T stands for the delayed signal $x(t-T)$, θ and τ are the characteristic times of the low and high cut–off frequency respectively, which are involved in the bandpass feedback filtering of the RF filter. From a signal processing viewpoint, such a dynamical system can be interpreted as a nonlinear delayed feedback oscillator. This oscillator is ruled by the dynamics of a linear bandpass filter $h(\omega)$, which is driven by a nonlinear transformation of two delayed "echos" (delays T and $T+\delta T$) of the filter output, $x(t)$. Chaotic solutions are obtained when the feedback loop gain β is high enough, of the order of 5. This gain is adjusted via the tuning of the laser light intensity. A typically observed chaotic solution is a white noise like signal which is covering the spectral range of the broadband bandpass feedback RF filter, *i.e.*, ca [30 kHz−13 GHz]. This results in a fast noise-like large amplitude signal $x(t)$, which is expected to be suitable for high speed RNG based on physical device. It is worth noticing that this chaotic signal generation process can be viewed as a balanced equilibrium between the RF feedback filter (limiting the spectral span of the signal $x(t)$), and the spectral broadening performed by the nonlinear transformation ($\sin^2$ −function of the difference delayed signals $x_T - x_{T+\delta T}$). The offset phase Φ_0 is typically adjusted through the static interference condition, which interference phenomena is physically at the origin of the $\sin^2$ nonlinear transformation.

A more accurate description of the generated signal $x(t)$ should also include (small amplitude) noise sources in the equation. The latter noise is actually of the same kind than the one involved in the noisy optoelectronic signal (laser and photodiode noise, also complemented here by the RF electronic amplifier noise). Equation (1) can be confidently used solely without the noise contribution, when the large amplitude chaotic motion only is of interest. To support this asumption, one might notice that such numerically obtained waveforms were found to exhibit very good qualitative agreement with the one observed in the experiment [33]. The proposed model has been also successfully used to derive analytically [34] most of the bifurcation features indeed observed in the experiment, thus indicating that the large amplitude solutions can be confidently calculated numerically from the noise-free model.

B. Extraction method for the random binary sequence

A schematic view of the algorithm used to extract a random binary sequence from a broadband physical signal, as proposed in [23], is depicted in Fig.2. On the basis of a physical setup delivering a broadband signal, as the one described in the previous section, a real time oscilloscope is first involved to perform an analogue to digital conversion of the output signal of the setup. This conversion is typically achieved via an 8-bit digitizer at a sampling rate of 40 GHz. In the next subsection, we will discuss from the signal theory viewpoint some particular processing issues that are found to significantly contribute to the actual randomness of the final binary sequence. More precisely, sampling issues will be discussed, quantization issues, and also post-processing operations (such as distant sample difference, and LSB-only retaining). This signal processing is performed before getting the actual final random binary sequence, to be tested for their randomness quality via standard statistical test suites.

1) Sampling issues: aliasing for enhanced entropy: In the following, we assume that samples are originally acquired by a real time digital scope measuring a broadband complex time trace. Such equipment is designed to follow the classical Shannon sampling theorem: the sampling rate f_S is matching the instrument analogue input bandwidth, which defines the maximum Fourier frequency f_M that can be captured by the instrument. The Shannon sampling theorem indeed states that a limited bandwidth signal can be digitized without loss of information, when the sampling frequency is at least twice the maximum signal frequency. The sequence of the samples $\{s_n = x(nT),\ n \in \mathbb{Z}\}$ can be defined as a function of the

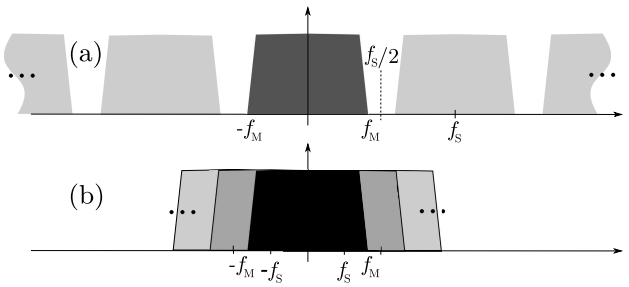


Fig. 3: Illustration of the properly fulfilled sampling theorem conditions (a), and the incorrect sampling condition leading to aliasing (b).

continuous time as follows:

$$s(t) = x(t) \cdot \text{⨿}_{T_S}(t), \tag{2}$$
$$\text{where } \text{⨿}_T(t) = \sum_{k=-\infty}^{k=+\infty} \delta(t - kT).$$

A typical illustration of the proof for the sampling theorem is presented in Fig.3, as one describes the spectrum of such a sampled signal $s(t)$,

$$S(\nu) = \text{FT}[s(t)] = X(\nu) \star \text{FT}[\text{⨿}_T(t)] = \frac{1}{T} X(\nu) \star \text{⨿}_{1/T}(\nu), \tag{3}$$

where we have used the well known result that the Fourier Transform (FT) of a comb is also a comb. The convolution product in the Fourier domain reveals that the spectrum of the sampled signal is the result of the superposition of an infinite number of regularly spaced replica of the original signal spectrum $X(\nu) = \text{FT}[x(t)]$, two neighboring replica being separated by the sampling frequency $f_S = 1/T$. Thus, if the maximum frequency f_M of the bounded support of $X(\nu)$ is less than $f_S/2$, the replicated spectra do not overlap (see Fig.3(a)). It is then obvious that a suitable window filtering of the sampled signal $s(t)$ allows to recover in the Fourier domain exactly the same spectrum as the one of the original signal $x(t)$. Such a filter typically transmits perfectly all the Fourier components in a frequency band such as $[-f_S/2, +f_S/2]$, and rejects all the other Fourier components for the other frequency ranges. When undersampling is used, the *aliasing* phenomenon occurs in the Fourier domain. It consists then of overlaps between the replicated spectra due to the comb convolution. The actual spectrum of the sampled signal $s(t)$, can be viewed as a complex mixing of the frequency components of the original signal $x(t)$, due to the overlapped replica of $X(\nu) = \text{FT}[x(t)]$. The procedure of selecting only one sample every n from the original sampled sequence, is thus equivalent to an aliasing operation with an undersampling of order n. The original goal of cementification of the extracted sample sequence, can thus be viewed as an aliasing technique resulting in a complex mixing of the original frequency components. The consequence is an increased entropy of the output sequence. When viewed in the time domain, this procedure results in the vanishing of the short time correlations, since a long time intervalle is then separating two successive samples, compared to the width of the autocorrelation function of the original signal. On the contrary, the short time scales correlations are necessarily present when the conditions of the sampling theorem are fulfilled (two successive samples would thus keep the information of short time scale correlations). Another consequence is that such an operation is unidirectional, in the sense that original information is actually lost after an aliasing process. Because of the complex mixing of the Fourier frequency components, the original spectrum cannot be recovered with a "simple" unmixing procedure.

2) Further post-processing: difference sequence between distant samples: In [22] and [23], computing the difference sequence between two neighbor samples are named as "derivative". However, mathematically speaking, the term "derivative" of $x(t)$ is used for the asymptotic value $(x(t+\Delta t) - x(t))/\Delta t$ when $\Delta t \to 0$. In the physical case of a finite sampling rate, the neighbor samples are obviously not infinitely close in time, hence we prefer not to use "derivative" here. More precisely, we are dealt here with significantly separated samples in time, since strong aliasing is first operated (see Section II-B1), with an undersampling number up to $n = 16$. The initial 40 GHz sampling rate is respecting the oscilloscope analogue input bandwidth of 12 GHz, but the final series obtained after retaining 1 sample over 16, is corresponding to a 2.5 GHz undersampling rate. The samples obtained after this distant sample difference (which will be called from here DSD) operation can be described as follows:

$$\{d_k^n\}_{k \in \mathbb{N}} = \{x[kT] - x[(k-n)T], k \in \mathbb{N}\}. \tag{4}$$

If we try again to analyze in the Fourier domain the meaning of this second processing, one obtain the following expression for the Fourier spectrum of $n-$undersampled difference signal:

$$D(\nu) = \left[2\, i\, e^{-i\pi\nu nT}\, X(\nu) \sin(\pi\nu nT)\right] \star \text{⨿}_{\frac{1}{nT}}(\nu). \tag{5}$$

This expression reveals a so-called channeled spectrum filter, which applies a periodic sinusoidal modulation of the original spectrum $X(\nu)$. One could notice that the maximum transmission of this filter is centered at half the undersampling rate ($(nT)^{-1}/2$) where aliasing is maximally symmetric (thus somehow selecting the frequency components that are most affected by aliasing), and the frequencies of null transmission are centered at zero and $\pm(nT)^{-1}$ (where the aliasing phenomenon is the less pronounced in the Fourier spectrum, as long as n is not too large). When focusing on the low frequency domain only, another comment about the action of this DSD processing could be made: the very low frequencies are filtered out, which consequence is to asymptotically set to zero the mean value of the corresponding sample set, and thus also improving the symmetry around zero of the amplitude probability distribution.

The Fourier analysis of the DSD processing is however not as obvious as for the aliasing issue in terms of randomness enhancement, or entropy amplification. A more meaningful discussion can however be made through the analysis of the statistical sample distribution of the DSD compared to the original one. More precisely, Fig.4a shows the evolution of the amplitude statistics when the DSD processing is iterated several times. One clearly sees that the statistics is more and more symmetric, resembling closer and closer to a Gaussian distribution. We have checked that introducing noise in the simulation does not change this result.

This convergence towards a Gaussian statistics through DSD can be qualitatively explained through the analysis of the DSD principle. Since the difference is performed between the same sample sequence but shifted in time over a quantity large

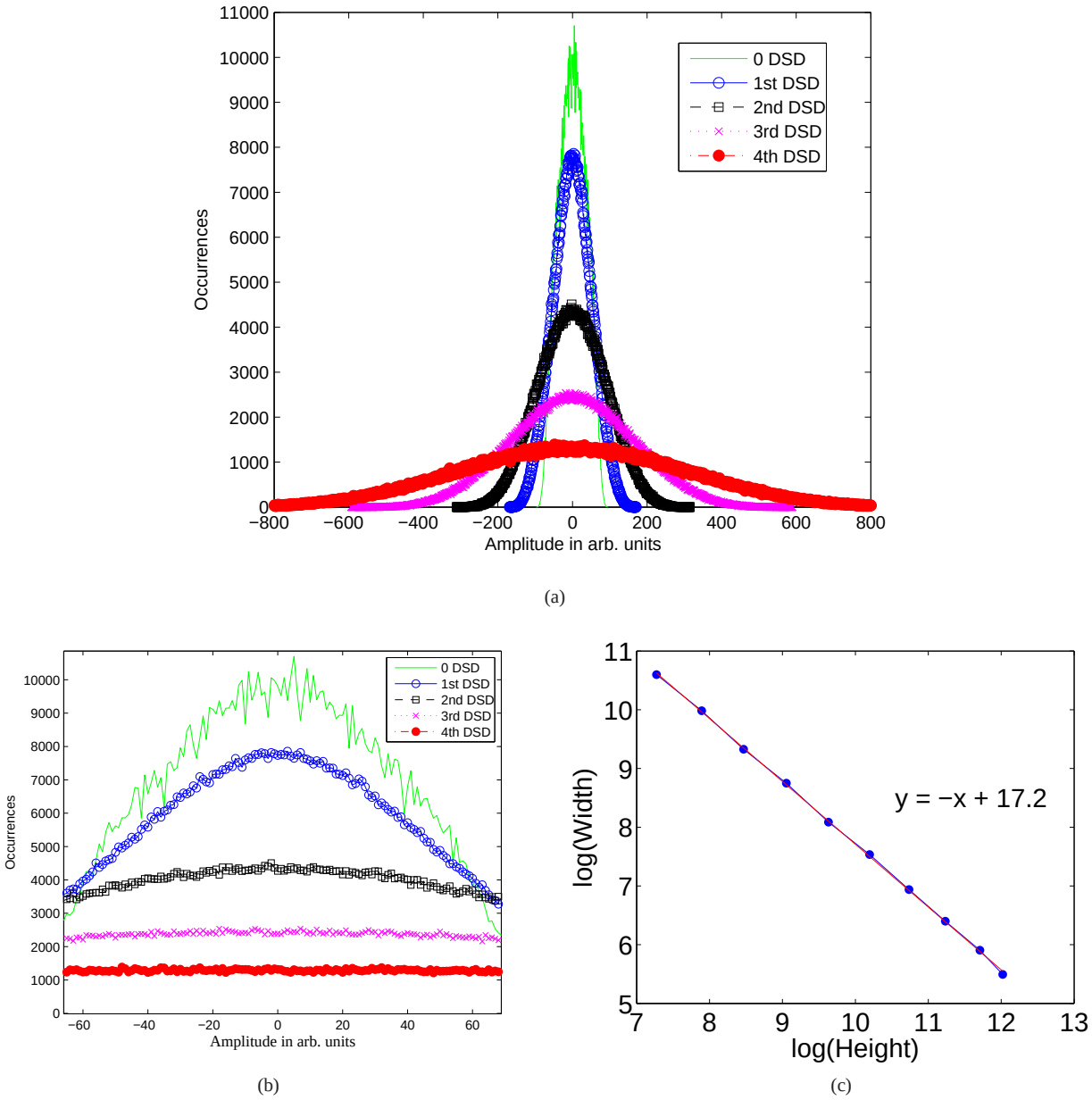


Fig. 4: Statistics of recorded chaotic time series (experimental). (a) 1st-4th times DSD for 2.5GHz undersampling; (b) Zooming of the centering area of (a); (c) 1st-10th times DSD, log-log plot between weight and height, showing the hyperbolic relationship between the two as DSD is repetitively processed.

enough compared to the correlation time, one can interprete the DSD as the superposition of nearly independent pseudo-random processes. The central limit theorem can then be used to explain qualitatively the amplitude distribution convergence towards a Gaussian one (limit of the amplitude distribution for the superposition of an asymptotically large number of independent random processes).

At the same time, as more and more DSD are operated, the amplitude range is increased along the horizontal axis, whereas the maximum of the statistics along the vertical axis is inversely decreased. Figure 4c shows the numerical evidence of a hyperbolic relation between width and height for the successive iterated processings.

This asymptotically Gaussian distribution obtained after a few DSD steps, finally prepares a kind of optimal statistical conditions for the last post-processing operation proposed by [22], leading to the final random bit sequence: LSBs retaining.

3) LSB retaining, and quantization noise effect: Surprisingly, the qualitative signal processing analysis of this last post-processing step, is involving very similar theoretical insight compared to the ones related to the aliasing phenomenon underlined in section II-B1. The main idea for the analysis of this last step of LSB retaining, actually originates from an elegant and powerful analogy between the temporal discretization occurring during sampling, and the amplitude discretization occurring as quantization is concerned [35]. Following the results of this statistical theory of quantization, one finds that the actual consequence of the LSBs retaining method is practically to provide a nearly constant (flat) amplitude probability distribution for the quantization noise, for quantization levels

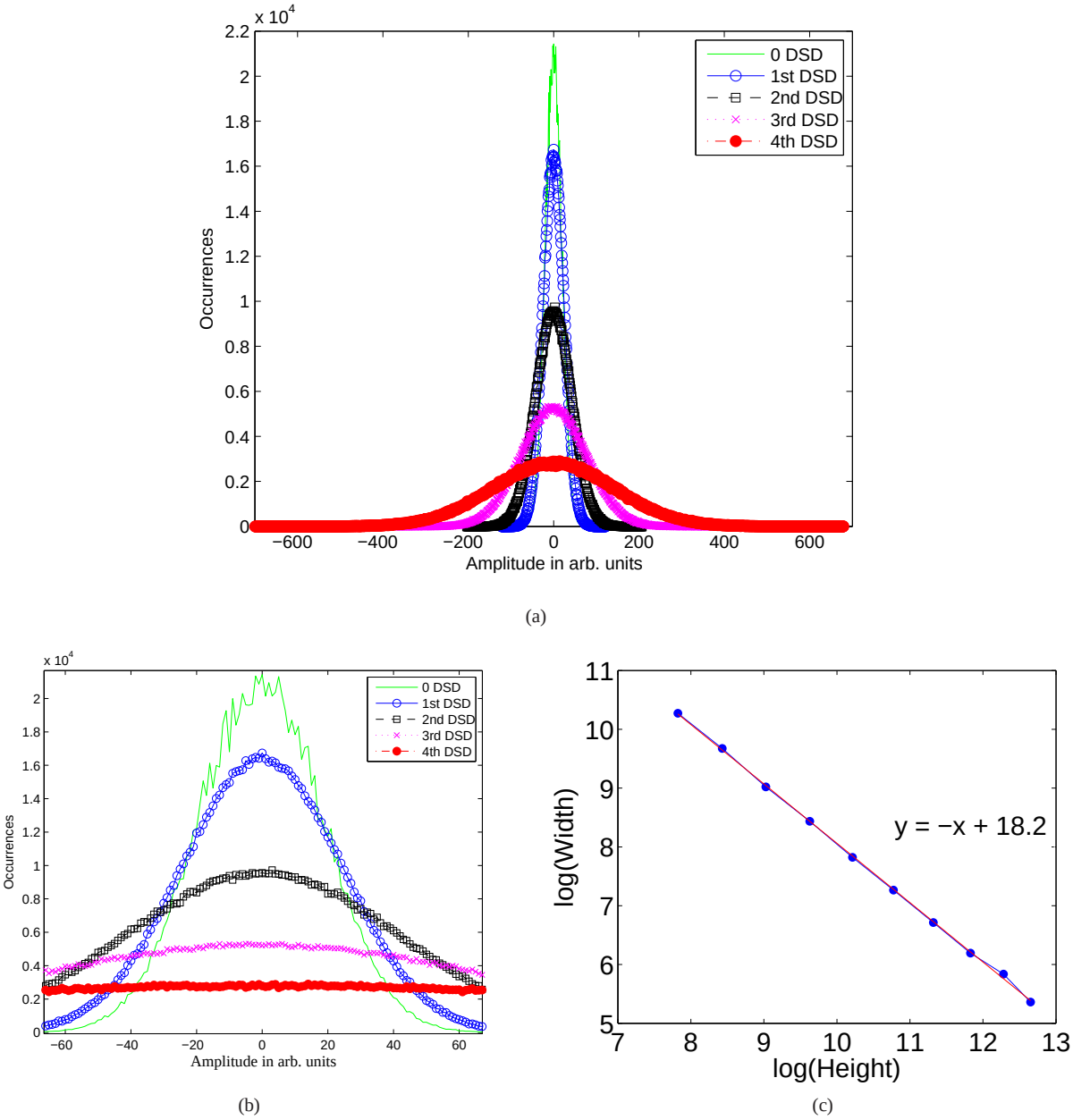


Fig. 5: Statistics of recorded noise time series (experimental). (a) 1st-4th times DSD for a 2.5GHz undersampling; (b) Zooming of the centering area of (a); (c) 1st-10th times DSD, the log-log plot between weight and height, showing the hyperbolic relationship between the two as DSD is repetitively processed.

as high as the root mean square of the signal to be quantized. In terms of LSBs retaining, this means that flat noise distribution is obtained for the corresponding LSBs amplitude, even if the LSB maximum amplitude reaches the root mean square of the quantized signal. As illustrated in Fig.9 of Ref. [35], the flat amplitude distribution results in a kind of aliasing from the original symmetric (Gaussian) amplitude distribution, which is segmented and superimposed over the central small amplitude interval limited by the resolution of the quantized amplitude (i.e. the amplitude range encoded by the retained LSBs).

Thus, after a complex mixing in the Fourier frequency domain due to a sampling theory aliasing effect, the LSB retaining process results in a strong flattening of the amplitude probability distribution for the retained LSBs. This flattening of the amplitude probability distribution can be also related to a kind of aliasing, but performed on the initial Gaussian amplitude probability distribution, according to the statistical theory of quantization. The Gaussian profile is implicitely provided through Reidler's method when a sufficiently high number of DSD processing is performed.

4) Discussion of the randomness origin: A straightforward issue can then be raised about the actual source of randomness leading to the final bit sequence, as proposed in [22]. The randomness origin has been many times attributed to the chaotic character of the solution generated by the original physical system: A SC laser diode subject to proper optical feedback, which is well known to exhibit chaotic motion. However, from the previously analyzed post-processing steps, no single argument related to any chaotic property of the original signal was involved. The only necessary requirement

was to have a certain broadband character in the original signal, such that first standard aliasing could occur in the Fourier domain. Second the DSD processing leads to a symmetrization of the amplitude statistics, with a convergence towards a Gaussian distribution. And last, LSBs retaining performs naturally a flattening of the final amplitude probability distribution corresponding to the selected bits.

To investigate this issue, we performed a similar analysis as the one done in the previous subsections on the chaotic motion of a nonlinear electro-optic delay dynamics, but with a physical signal a priori originating from physical noise sources only, without any deterministic chaotic compound. This signal is chosen to be the output of the amplified photodiode of the same setup, but without the nonlinear delayed feedback loop at the origin of the chaotic time series: The amplified photodiode signal is issued from the laser intensity noise, it comprises also the photodiode junction noise and the electronic amplifier noise (see "Optoelectronic Noise" output in Fig.1). Although the electrical signal level is significantly lower, we used the scope magnification to get a time trace of a comparable amplitude with respect to the scope vertical amplitude range, thus resulting in an effective digital scope quantization over a comparable number of bits with respect to the chaotic signal.

We have reported in Fig.4 and 5 the statistics evolution of the digitally acquired optoelectronic noise signal and its width / height evolution. The figures clearly show very similar features. From this rough analysis of the influence of the two physical signals (the optoelectronic noise and the electro-optic chaos), we realize that the post-processing leads to qualitatively equivalent final bit sequence. This observation, and the previous analysis of the post-processing steps, support the assumption, at least qualitatively, that the randomness of the final bit sequence might be mainly issued from the post-processing steps. The chaotic feature of a time series appears as an actually sufficient but not required condition, for the generation of a random bit sequence when the discussed post-processing is used (undersampling, DSD, and LSBs retaining). A simple noisy signal with similar spectral extend is found to lead to similar final output bit stream, as already reported previously [4], but not yet analyzed and interpreted as we have proposed.

III. Effect of Noise on the Entropy Rate in the Binary Sequence

In this section, the time evolution of the entropy in the final binary sequence is evaluated under different choices for the method used to build the final random bit stream from the chaotic signal. The aim is to get insight in the origin of the entropy creation mechanism involved in the construction of the final random bit stream. More precisely, we aim at discriminating under which conditions the deterministic feature of the chaotic signal (the determinism coming from the dynamics described by Eq.(1)) is indeed involved in the entropy of the extracted bit stream. To achieve this goal we reproduce the method proposed in [36], which is intended to measure the sensitivity to initial condition (SIC) of the deterministic chaotic motion in the presence of additional small noise. This measure consists in calculating the temporal entropy evolution for the generated binary random sequence, with respect to several different noise realizations.

A. Introducing noise in the simulated chaotic dynamics

For the entropy calculation, we first consider a transient-free chaotic solution of Eq.(1) ($\beta = 5$). To achieve such a solution, Eq.(1) is integrated under the proper parameter conditions known to lead to a high complexity chaotic solution. This preliminary numerical integration is performed over a duration long enough compared to the slowest characteristic time scale of the dynamics (θ), so that the asymptotic trajectory is free of any transient. Once this corresponding chaotic attractor is supposed to be reached via the numerical integration, this asymptotic solution can be associated to a single temporal waveform covering only the longest time delay of the dynamics, i.e. $T + \delta T$: this is defining the initial condition of the corresponding delay based, and noise-free, chaotic dynamics, from which noise influence will be explored. We then introduce in the right hand side of Eq.(1) an arbitrary small additive noise term (small perturbation along the chaotic trajectory). The noise amplitude is arbitrarily set so that the Signal-to-Noise Ratio (SNR) is 40 dB. After further integrating Eq.(1) with the noise term and starting from the initial condition corresponding to the calculated noise free chaotic trajectory, one is able to obtain a continuously noise-perturbed chaotic trajectory. When repeating this calculation with several different noise realizations, one then expects to observe the effect of SIC when comparing the different noise perturbed chaotic trajectories. This property manifests itself through a progressive amplification (as time is running) of the small perturbations materialized by the added noise. Comparing the different calculated waveforms, they consequently looks all the same right after the noise addition, but they split apart (differently for each pair of such time series) after a typical time scale related to the inverse of the largest Lyapunov exponent of the chaotic dynamics (see Ref. [36] for details). Two such simulated waveforms are represented in Fig.6, after the undersampling procedure, and before the DSD and bit retaining processes for the final extracted binary sequence. The waveforms thus do not appear anymore as continuous in time due to undersampling. For these two realizations and with the chosen SNR for the noise amplitude, one clearly sees that the two time series separate one from each other after a typical time scale of ca. 300 ns. This time scale is of the order a few tens of the largest time delay $T + \delta T$, which is corresponding to a few tens round trips of the chaotic signal in the nonlinear delayed feedback loop. This is fully consistent with the typical order of magnitude of the inverse largest Lyapunov exponent, i.e. it is of the order of the largest time delay in the dynamics.

B. Entropy estimation for each bit cell

Many different noisy chaotic time series ($N = 10^3$) are simulated to generate as many random bit sequences. Each realization is calculated from the same initial conditions (the noise free chaotic waveform over one largest delay time interval), but with different added small noise perturbations. From each obtained time series, one can explore various bit stream extraction methods, e.g. with or without DSD, or even with several successive DSD processing, with the LSB retaining or with the MSB, ... For a fixed bit extraction method, the N obtained bit sequences can be used to calculate, at each time t_k of a new extracted bit, the probabilities $P_0(t_k)$ and

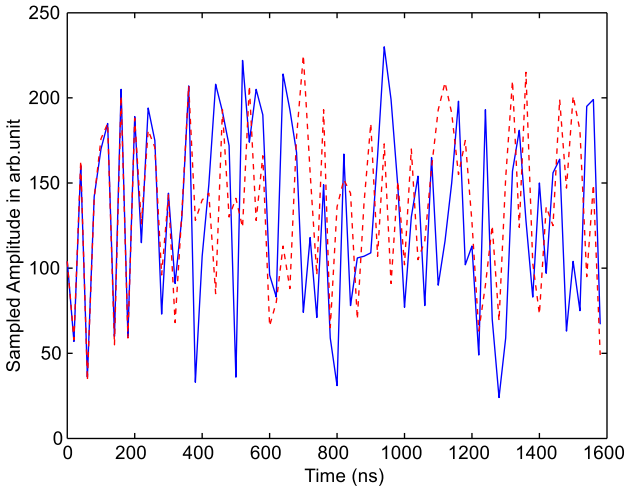


Fig. 6: Two simulated waveforms of chaotic laser intensity starting from the same initial conditions with different noise sequences added at time 0. The noise amplitude is set so that SNR is 40 dB (the signal energy being calculated on the noise-free chaotic trajectory)

$P_1(t_k)$ for obtaining a bit 0 or 1 respectively. This time varying probability distribution is then used to calculate how the statistical bit entropy evolves in time,

$$H(t) = -\sum_{i=0}^{1} P_i(t) \cdot \log_2 P_i(t). \tag{6}$$

As described in [36] if SIC of a chaotic dynamics is indeed involved in the final bit sequence, the N extracted bit sequences are initially strongly correlated. This is because the bits are originating from the same initial chaotic waveform. Consequently, the influence of the small added noise is negligible at the initial times of the deterministic chaotic dynamics: the entropy at small t is expected to be close to zero if indeed the dominating phenomena is deterministic. However, as time is evolving, SIC is amplifying the influence of the small noise amplitude on the large amplitude chaotic motion, and the N bit streams realizations are more and more decorrelated, leading progressively to a maximum binary entropy of 1. This unity entropy means an equal probability for obtaining bit zero and one, independently of any deterministic motion. The influence of the small added noise term is then dominating the output random bit stream. One should notice here that the bit extraction method used in Ref. [36] concerns MSB only. In our case, we apply the complex bit extraction method with multiple steps (aliasing, DSD, LSBs retaining) proposed in [22], and we are interested in the resulting entropy growth rate under these particular conditions, with actually expected significant differences.

Figure 7 represents the obtained binary entropy calculated with different bit extraction methods. In the first column, the binary entropies obtained from a direct 8-bits ADC for different bits from LSB to MSB, are plotted as a function of time. According to the description of [36], memory time is defined as the time required for the entropy to reach a value close to one. One clearly sees that as the bits chosen for the random bit stream moves from LSB to MSB, the memory time of the related bit cell is increasing. This illustrates that MSBs are most reflecting the deterministic features of the signal, whereas this determinism is earlier lost as smaller LSBs are concerned: The SIC amplification of the small initial differences (noise realizations in that case) occurs naturally earlier for LSBs than MSBs. Differently speaking, this illustrates the fact that deterministic properties are more prononced with MSBs, or equivalently, LSBs are containing less deterministic features than MSBs.
Columns 2 and 3 in Fig.7 are showing similarly this determinism loss from MSBs to LSBs, when one and two DSD steps are processed respectively. One clearly sees that the smooth entropy transition, which is a signature of the chaos determinism, even completely disappears for LSBs (a zoom-in over the first ns, would show that the entropy already starts at values very close to unity).

The conclusion on Fig.7 is that fastest entropy rate (down to the actual sampling) can be achieved when LSBs are used and when several DSD processing are performed. This is however achieved at the cost a full lost of determinism (zero memory time, without any smooth entropy growth). This corresponds to the plots on the upper right positions, for which unit entropy is already achieved very close to the time origin. This support the fact that deterministic chaos does not exist anymore in the obtained final bit stream randomness.
On the contrary, the MSBs are showing a non-zero memory time, and thus a signature of a maintained determinism. The most pronounced determinism is revealed in the lower left plots, for MSB and without any DSD. One could notice that this actually corresponds to the 1-bit ADC used in [9], where deterministic chaotic origin does contribute to the randomness of the final bit stream. In this case, the good randmoness quality is obtained only by carefully combining two uncorrelated chaotic signals (two chaotic lasers, with incommensurate characteristic time scales).

Figure 8 shows the plots of every bit cell entropy averaged over 10^3 trajectories. Each plot of entropy is obtained as a function of time for an ensemble of time series starting with exactly the same initial condition at time $t = 0$. Eight plots are shown in Fig. 8 corresponding to eight different position bit cell of the value. These curves are the smoothed versions, due to averaging, of the curves represented in the first column of Fig.7. Again, it can be seen that more time is required to converge to a unity entropy when using MSB compared to the use of LSB. Differently speaking, the memory time depends on bit cell selecting, MSB and LSB appearing as the slowest and fastest entropy increasing rate, respectively.

IV. Statistical Tests

Additionally to the previous signal theory analysis of the processing steps used in the bit extraction method, this section is intended to qualify the final bit stream in terms of their benchmarking from several standard randomness test suites. We thus verify in this section that the analyzed and used method proposed in [22] and [23] have led also in our experiment to quasi-equivalent random bit stream quality, whether from the deterministic EO phase chaos generator or with the optoelectronic noise source.

A. The tested streams

First of all, we give here a brief description of the tested methods that have been formerly proposed in [22] and [23].

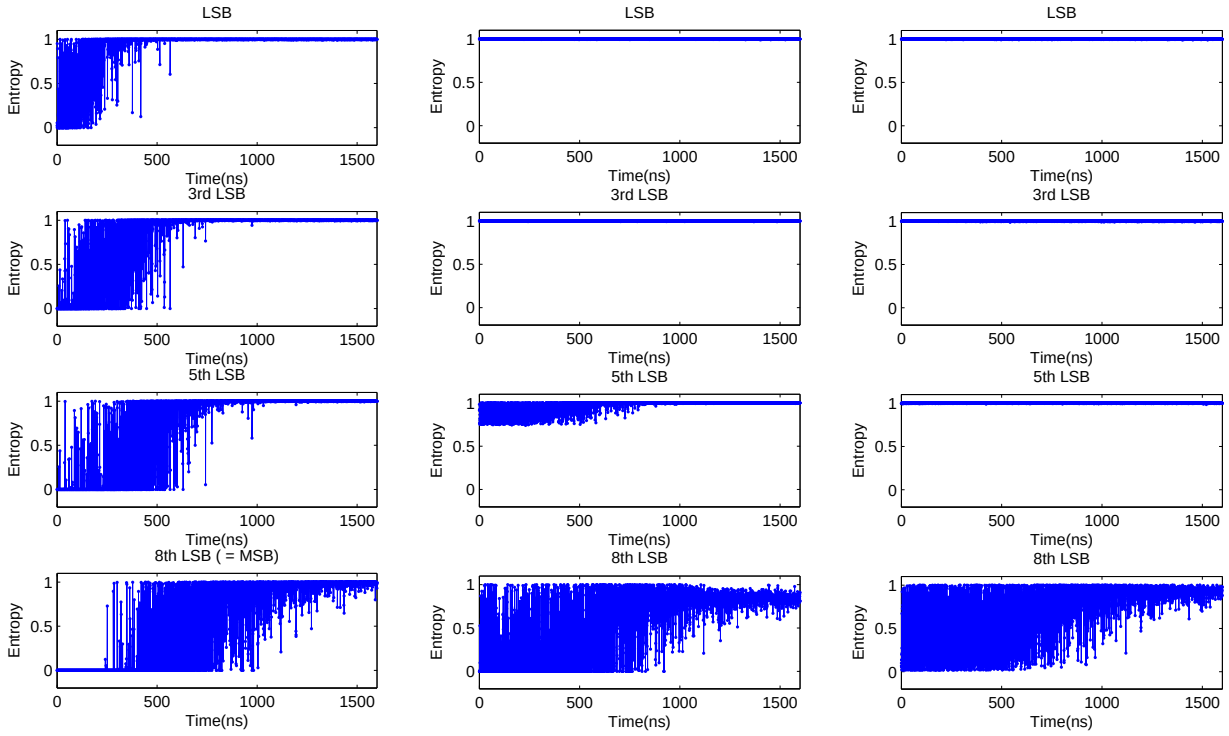


Fig. 7: LSBs entropy evolution as a funtion of time, for an ensemble of simulated chaotic time series with the same initial conditions, but with different small noise added to it. The noise strength is -40 dB, with sampling rate 2.5 GHz 8-bit ADC. (a) For sampling value; (b) For the 1st DSD of the sampling value. (c) For the 2nd DSD of sampling value.

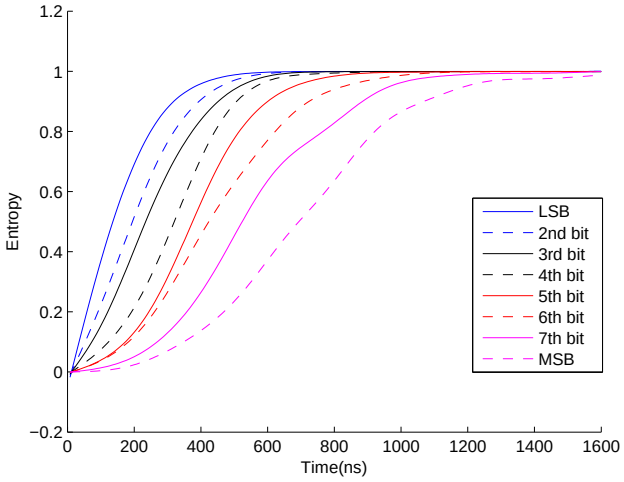


Fig. 8: Simulated averadge growth of bit entropy and its dependence on bit cell selecting (from MSB to LSB), without any DSD

On the one hand, in [22], authors have used a DSD method to generate a random bits stream. The chaotic laser signal is sampled by using a 2.5 GHz ADC, and then 5 LSBs of every first DSD value are joined together to generate the final random sequence. On the other hand, in [23], the chaotic laser signal is sampled thanks to a 20 GHz ADC. Then the DSD operation is processed 4 times and 8 LSBs of each value are joined to produce the pseudorandom bit stream.

These two schemes are both adapted to optoelectronic noisy signal. The generated streams sourced from chaotic laser and noise are compared by standard statistical tests in the next subsections.

B. Statistical tests

Considering the properties of binary random sequences, various statistical tests can be designed to evaluate the assertion that the sequence is generated by a perfectly random source. We have performed some statistical tests for the optoelectronic noise and electro-optic chaos generators proposed here. These tests include NIST suite [37], DieHARD battery of tests [38], ENT program [39], and and some comparative test parameters. A brief description of each of the aforementioned tests is given in the following paragraphs.

1) NIST statistical test suite: Among the numerous standard tests for pseudorandomness, a convincing way to show the randomness of the produced sequences is to confront them to the NIST (National Institute of Standards and Technology) Statistical Test, because it is an up-to-date test suite proposed by the Information Technology Laboratory (ITL). A new version of the Statistical Test Suite has been released in August 11, 2010.

The NIST test suite SP 800-22 is a statistical package consisting of 15 tests. They were developed to test the randomness

of binary sequences produced by hardware or software based cryptographic pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence.

For each statistical test, a set of $P-values$ (corresponding to the set of sequences, $\mathbb{P}_T$) is produced. The interpretation of empirical results can be conducted in various ways. In this paper, the examination of the distribution of $\mathbb{P}_T$ to check for uniformity is used. The distribution of P-values is examined to ensure uniformity. If $\mathbb{P}_T \geqslant 0.0001$, then the sequences can be considered to be uniformly distributed.

In our experiments, 100 sequences ($s = 100$), each with 1,000,000-bit long, are generated and tested. If the $\mathbb{P}_T$ of any test is smaller than 0.0001, the sequences are considered to be not good enough and the generating algorithm is not suitable for usage. In Table I, the random streams generated by the chaotic laser and by the noisy signal have both obtained a 100% passing rate when considering the NIST battery of tests, thus it is impossible to found a difference between the two streams using the NIST suite.

2) DieHARD battery of tests: The DieHARD battery of tests has been the most sophisticated standard for over a decade. Because of the stringent requirements in the DieHARD test suite, a generator passing DieHARD battery of tests can be considered good as a rule of thumb.

The DieHARD battery of tests consists of 18 different independent statistical tests. This collection of tests is based on assessing the randomness of bits comprising 32-bit integers obtained from a random number generator. Each test requires 2^{23} 32-bit integers in order to run the full set of tests. Most of the tests in DieHARD return a $P-value$, which should be uniform on $[0, 1)$ if the input file contains truly independent random bits. Occasional $P-value$s near 0 or 1, such as 0.0012 or 0.9983 can occur. However, an individual test is considered to be failed if its $P-value$ approaches 1 closely, for instance, $P - value > 0.9999$.

Results derived from applying the DieHARD battery of tests to the two random streams computed from experimental time series, reveals that both sequences can pass sucessfully all the tests. This confirms that the quantitative randomness of the bit stream taken from the chaotic laser intensity indicates similar features compared to the one obtained by the optoelectronic noise source (thus without any chaotic origine).

3) ENT test program: ENT test program applies various tests to sequences of bytes stored in files and reports the results of those tests. The program is useful for evaluating random number generators for encryption and statistical sampling applications, compression algorithms, and other applications where the information density of a file is of interest [39].

There are 5 tests contained in the program:

1) Entropy test: Entropy in bits per character (or byte), which corresponds to the incompressibility of the sequence (as a perfectly random sequence cannot be compressed, since no part of it can be expressed in terms of other parts). Hence entropy of 8 bits/byte means perfect randomness in the sense of incompressibility.
2) χ^2 test: χ^2 testing is very common for goodness-of-fit of sample distributions of random numbers. It is known to be very sensitive to deficiencies in random number generators (when it is located between 5% to 95%, data are treated as random).
3) Sample test: Sample test means can be tested for bias in random number generation. In binary mode, the expected mean is 0.5 while for bytes, the expected mean is 127.5.
4) Monte Carlo test: a Monte Carlo approximation of π, which is simply the evaluation the area of the unit circle using the N generated random numbers (X_i,X_{i-1}), $i = 2, ..., N$.
5) Serial Correlation test: Serial correlation coefficient evaluated from $< X_i, X_{i-1} > / < X_i, X_i >$, for $i = 2, ..N$. The intended value for perfect random sequences is 0.

In Table II, it is shown that the results for each pair of random streams, considering these five tests detailed above, are very closed one to each other. They all achieved to pass the threshold of the Chi-squared test, and the results are very similar for the other tests. To sum up, all these streams satisfy the same random-like behavior according to the ENT battery.

4) Comparative test parameters: Five well-known statistical tests [40] are used too as simple comparison tools. They encompass frequency and autocorrelation tests. In what follows, $s = s^0, s^1, s^2, \ldots, s^{n-1}$ denotes a binary sequence of length n. The question is to determine whether this sequence possesses some specific characteristics that a truly random sequence would be likely to exhibit. Standard tests intended to answer this question are *Frequency test (monobit test)*, *Serial test (2-bit test)*, *Poker test*, *Runs test* and *Autocorrelation test* (we refer the reader to [40] or [41] for detailed definitions).

We show in Table III a comparison between two random bits streams sourced respectively by the chaotic laser intensity and by the noisy optoelectronic signal. The results confirm that the proposed random streams present very closed statistical qualities. This finding implies that to have a chaos-like deterministic origin is not a required condition for high randomness quality in the proposed method.

Finally a comparison of the overall stability from 5×10^3 to 2×10^5 for these generators is given in Fig. 9. It can be seen that the trends for the amplitude movements of values are more or less in the same scale, which again indicates that all these random sequences share closed random properties.

V. Discussion, Conclusion, and Perspectives

Random number generation via photonic broadband signal generation does provide nowadays a novel and interesting approach allowing for unprecedented high bit rate of random bit streams. These photonics to digital world conversion are designed so that randomness can be certified according to most of the usual randomness tests such as NIST and DieHARD suites. Among the recently proposed physical systems and related processing intended to extract bit streams from photonic analogue waveforms, two rather different approaches can be identified: when the source of randomness explicitly stems from photonic noise [4]–[6], and when deterministic chaos is claimed to be at the origin of the random bit stream [9], [22]. Whereas the first approach provides obviously, and by definition, a non deterministic random bit stream, the second one has an implicit potential source of determinism, similarly to the algorithmic and fully digital pseudorandom bit sequence (PRBS) generators.

A major interest of the digital PRBS resides in their capability of generating a distant and synchronized random bit stream, which allows one to apply them in symmetric cryptography.

TABLE I: NIST SP 800-22 test results ($\mathbb{P}_T$)

Method	2.5GHz, 1st DSD, 5LSB		20GHz, 4th DSD, 8LSB	
Source	Chaotic laser	Noise	Chaotic laser	Noise
Frequency:	0.935716	0.798139	0.171867	0.834308
BlockFrequency:	0.040108	0.350485	0.289667	0.867692
CumulativeSums:	0.334152	0.575225	0.228927	0.688782
Runs:	0.595549	0.834308	0.851383	0.637119
LongestRun:	0.191687	0.964295	0.162606	0.304126
Rank:	0.534146	0.037566	0.637119	0.719747
FFT:	0.236810	0.514124	0.202268	0.249284
NonOverlappingTemplate:	0.502510	0.491449	0.521769	0.501830
OverlappingTemplate:	0.851383	0.964295	0.090936	0.574903
Universal:	0.798139	0.739918	0.102526	0.319084
ApproximateEntropy:	0.224821	0.236810	0.435436	0.419021
RandomExcursions:	0.347389	0.229729	0.471174	0.104312
RandomExcursionsVariant:	0.217344	0.209317	0.461569	0.350467
Serial:	0.300289	0.366918	0.237996	0.606177
LinearComplexity:	0.350485	0.262249	0.224821	0.935716

TABLE II: ENT battery using 10^8 bits for each stream

Method	Using source	Entropy	Chi-square	Sample	π error	Correlation
2.5GHz, 1st	Chaotic laser	7.999984	67.18%	127.4988	0.03%	-0.000771
DSD, 5 LSBs	Noisy signal	7.999986	7.13%	127.5034	0.03%	-0.000392
20GHz, 4th	Chaotic laser	7.999986	73.48%	127.4973	0.03%	0.000481
DSD, 8 LSBs	Noisy signal	7.999985	12.37%	127.5011	0.02%	-0.000411

TABLE III: Comparison between the presented sources for a 2×10^7 bits sequence

Subjects	Monobit	Serial	Poker	Runs	Autocorrelation
Method	2.5GHz, 1st DSD, 5LSBs				
Chaotic laser	0.2509	1.9200	16.6650	16.6215	1.5739
Noise	0.6019	0.7144	8.5606	17.5156	1.5247
Method	20GHz, 4st DSD, 8LSBs				
Chaotic laser	1.4580	0.5199	13.1430	28.9460	1.1583
Noise	0.2554	0.7835	14.0035	22.9136	1.6739

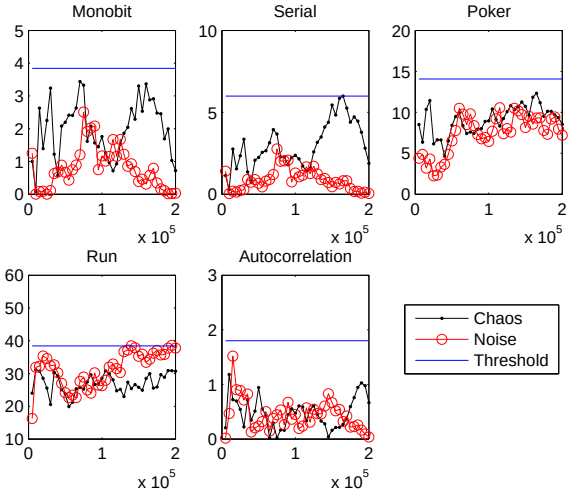
A major advantage of PRNG is precisely their perfect determinism, and perfect control, due to their digital program-based generation process. This feature is also at the origin of their main drawback: the same absolute digital determinism can be used in principle for cryptanalysis, trying to guess the seed which can then deterministically and totally allow for the random bit sequence reproduction, even by an eavesdropper. Also from a more technical viewpoint, the processor based architecture of PRNGs defines some speed limitations related to the processor clock, and the number of elementary operations needed to implement the PRNG algorithm. Noise based, and chaos based, photonic RNGs provide at least a technical answer to the limited bit rate generation provided by purely algorithmic solutions. It was also reported in many attempts on photonics based RNGs, that high quality randomness is possible, since they can pass successfully all the standard NIST and DieHARD test suites. A strong open problem however still remains concerning the capability to control, and reproduce, the random bit stream provided by photonic chaos-based RNGs. On the contrary to the photonic noise based RNGs, this indeed can be expected from the chaos-based photonic RNGs, since they also originates, at least partially, from deterministic dynamics, similarly to the algorithmic PRNGs.

In that particular context, we have proposed to address related issues, through the analysis of a particular post-processing method [22] applied in many chaos-based photonic RNGs. The actual role of deterministic chaos in this photonic RNG approach was known to be controversial [4], [42] (but not analyzed), since purely non-deterministic (noisy) photonic signals were found to lead to similar randomness quality when using the same method.

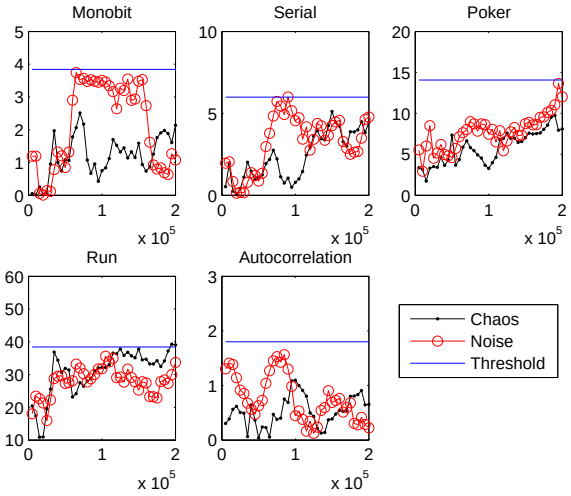
In this article, we have checked on additional experiments that the proposed method can succesfully lead to high speed and high randomness quality, whether when used on strongly deterministic chaos provided by an electro-optical phase dynamics, or when used on a photonic noise having comparable spectral and statistical features. It is thus confirmed that chaos is not a necessary condition for the method to be successful.

We have also analyzed and interpreted this digital post-processing method. Standard signal theory arguments revealed that the method is actually acting as an entropy enhancement through aliasing phenomena, both with the time discretization (undersampling) and with the amplitude discretization (LSBs retaining).

Finally, we have also investigated how a typical signature of deterministic chaos, sensitivity to initial condition, can or



(a) 2.5GHz, 1st DSD, and 5 LSB method



(b) 20GHz, 4th DSD, and 8 LSB method

Fig. 9: Overall Sequence Stability Comparison

cannot survive in the final bit stream. It is found that this determinism signature is actually lost precisely due to the random bit stream extraction method.

We also conclude that the analyzed bit stream extraction method does not appear as suitable, when further use of deterministic feature is expected. For example, this happens when one wants to achieve synchronization between distant random bit stream (e.g. when cryptographic applications are concerned, such as one time pad cypher).
Synchronizable random bit stream generated from deterministic chaos, is thus still an open problem, which would require other bit stream extraction methods able to provide both a strong enough determinism together with a high randomness quality.

Acknowledgement: This work was supported by the European project PHOCUS (FP7 grant 240763), and by the Labex ACTION program (contract ANR-11-LABX-01-01).

REFERENCES

[1] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge Univ. Press, 2000.
[2] R. Gallager, *Principles of Digital Communication*. Cambridge University Press, 2008.
[3] D. Stinson, *Cryptography: Theory and Practice*. CRC Press, 1995.
[4] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Optics Express*, vol. 18, pp. 23584–23597, November 2010.
[5] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent led," *Optics Letters*, vol. 36, pp. 1020–1022, March 2011.
[6] B. Wetzel, K. J. S. K. Blow, K. J. Turitsyn, G. Millot, L. Larger, and J. M. Dudley, "Random walks and random numbers from supercontinuum generation," *Optics Express*, vol. 20, pp. 11143–11152, May 2012.
[7] T. Yamazaki and A. Uchida, "Performance of random number generators using noise-based superluminescent diode and chaos-based semiconductor lasers," *IEEE J. Select. Top. Quantum. Electron.*, vol. 19, p. 0600309, August 2013.
[8] T. Stojanovski and L. Kocarev, "Chaos-based random number generator part i: Analysis," *IEEE Trans. Circuits Syst. I*, vol. 48, pp. 281–288, March 2001.
[9] A. Uchida, K. Amano, I. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol. 2, pp. 728 – 732, 2008.
[10] T. E. Murphy and R. Roy, "Chaotic lasers: The world's fastest dice," *Nature Photonics*, vol. 2, pp. 714 – 715, 2008.
[11] K. Hirano, K. Amano, A. Uchida, S. Naito, M. Inoue, S. Yoshimori, K. Yoshimura, and P. Davis, "Characteristics of fast physical random bit generation using chaotic semiconductor lasers," *IEEE J. Quant. Electron.*, vol. 45, no. 11, pp. 1367 – 1379, 2009.
[12] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.
[13] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and A. K. Shore, "Chaos–based communications at high bit rates using commercial fiber–optic links," *Nature*, vol. 438, pp. 343–346, 2005.
[14] J. Bahi, X. Fang, and C. Guyeux, "An optimization technique on pseudorandom generators based on chaotic iterations," in *INTERNET'2012, 4-th Int. Conf. on Evolving Internet*, (Venice, Italy), pp. 31–36, June 2012.
[15] "Randomness requirements for security," *http://tools.ietf.org/html/rfc4086*, Last check in 2011.
[16] J. Walker, "Hotbits: Genuine random numbers, generated by radioactive decay," *http://www.fourmilab.ch/hotbits/*, Last check in 2011.
[17] G. Bernstein and M. M.Lieberman, "Sercure random number generation using chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. 37, pp. 1157 – 1164, 1990.
[18] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouvo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card ic," *IEEE Trans. Comput.*, vol. 52, pp. 403 – 409, 2003.
[19] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Applied Physics Letters*, vol. 93, no. 3, p. 031109, 2008.
[20] G. Taylor and G. Cox, "Digital randomness," *IEEE Spectrum*, Sept. 2011.
[21] T. Mukai and k. Otsuka, "New route to optical chaos: Successive-subharmonic-oscillation cascade in a semiconductor laser coupled to an external cavity," *Physical Review Letters*, vol. 55, pp. 1711–1714, 1985.
[22] I. Reidler, Y. Aviad, M. Rosenbluh, and I. Kanter, "Ultrahigh-speed random nuber generation based on a chaotic semiconductor laser," *Physical Review Letters*, vol. 103, pp. 24 – 28, Jul 2009.
[23] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, "An optical ultrafast random bit generator," *Nature Photonics*, vol. 4, no. 1, pp. 58 – 61, 2010.
[24] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, and D. Syvridis, "Implementation of 140 gb/s true random bit generator based on a chaotic photonic integrated circuit," *Optics Express*, vol. 18, pp. 18763–18768, August 2010.
[25] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals,," *IEEE J. Lightwave Technol.*, vol. 30, pp. 1329–18768, May 2012.
[26] N. Oliver, M. C. Soriano, D. W. Sukow, and I. Fischer, "Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation," *Optics Letters*, vol. 36, pp. 4632–4634, December 2011.
[27] M. R. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," *Optics Express*, vol. 20, pp. 25333–25344, November 2012.
[28] M. R. Nguimdo, G. Verschaffelt, J. Danckaert, X. Leijtens, J. Bolk, and G. Van der Sande, "Fast random bits generation based on a single chaotic semiconductor ring laser," *Optics Express*, vol. 20, pp. 28603–28613, December 2012.

[29] X.-Z. Li and S.-C. Chan, "Random bit generation using an optically injected semiconductor laser in chaos with oversampling," *Optics Letters*, vol. 37, pp. 2163–2165, June 2012.
[30] P. Li, Y.-C. Wang, A.-B. Wang, L.-Z. Yang, M.-J. Zhang, and J.-Z. Zhang, "Direct generation of all-optical random numbers from optical pulse amplitude chaos," *Optics Express*, vol. 20, pp. 4297–4308, February 2012.
[31] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Optics Express*, vol. 18, pp. 23584–23597, November 2010.
[32] R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 gb/s chaos communications," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1430–1435, 2010.
[33] R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. S. Udaltsov, and J. M. Dudley, "Electro–optic delay oscillator with non–local non linearity: optical phase dynamics, chaos, and synchronization," *Phys. Rev. E*, vol. 80, p. 026207, 2009.
[34] L. Weicker, T. Erneux, M. Jacquot, Y. Chembo, and L. Larger, "Crenelated fast oscillatory outputs of a two-delay electro-optic oscillator," *Phys. Rev. E*, vol. 85, p. 026206, 2012.
[35] B. Widrow, I. Kollár, and M.-C. Liu, "Statistical theory of quantization," *IEEE Trans. Instrum. Meas.*, vol. 45, pp. 353–361, Apr. 1996.
[36] T. Mikami, K. Kanno, K. Aoyama, A. Uchida, T. Ikeguchi, T. Harayama, S. Sunada, K.-i. Arai, K. Yoshimura, and P. Davis, "Estimation of entropy rate in a fast physical random-bit generator using a chaotic semiconductor laser with intrinsic noise," *Phys. Rev. E*, vol. 85, p. 016211, Jan 2012.
[37] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," *NIST Special Publication 800-22*, 2010.
[38] "Diehard test suite," *http://www.stat.fsu.edu/pub/diehard/*, Last check in July 2011.
[39] J. Walker, "Ent: a pseudorandom number sequence test program," *http://www.fourmilab.ch/random/*, Last check in July 2011.
[40] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, and R. L. Rivest, *Handbook of applied cryptography*. CRC Press, 1997.
[41] J. M. Bahi, F. Xiaole, C. Guyeux, and W. Qianxue, "Randomness quality of ci chaotic generators: Applications to internet security," *2nd International Conference on Evolving Internet*, 2010. http://dx.doi.org/10.1109/INTERNET.2010.30.
[42] K. Hirano, T. Yamazaki, S. Morikatsu, H. Okumura, H. Aida, A. Uchida, S. Yoshimori, K. Yoshimura, T. Harayama, and P. Davis, "Fast random bit generation with bandwidthenhanced chaos in semiconductor lasers," *Optics Express*, vol. 18, pp. 5512–5524, March 2010.

Xiaole Fang received his PhD degree in March 2013 in Computer Science and Engineering, at the department of complex system (DISC), FEMTO-ST Institute, University of Franche-Comt, supervised by Professors Jacques Bahi and Laurent Larger. The main objective of his thesis is to explore different possible approaches efficiently (in terms of speed and quality of randomness) to extract pseudo-random number sequence by adapting new mathematical topology properties. Before arriving in University of Franche-Comt, he completed two postgraduate studies: Master of Science in Theory and Engineering of Control (2006-2008) and Electronics and Electrical Engineering Systems (2009). Since 2010, he has published 1 articles in international journal, and 4 articles in peer reviewed international conferences.

Benjamin Wetzel was born in Besançon, France in 1986. He received his MSc and Ph.D. degree in optics and photonics from University of Franche-Comté, Besançon, France in 2009 and 2012, respectively. His MSc research held in Tyndall National Institute, Cork, Ireland, was focused on semiconductor laser injection stabilities and dynamics. His Ph.D research was carried out in FEMTO-ST Institute where he studied, nonlinear dynamics and instabilities in optical fiber propagation, supercontinuum generation as well as complex dynamical systems. In 2013, he started a postdoctoral position in FEMTO-ST where he is currently working on femtosecond ablation, non-diffracting beams spatial shaping and graphene photonics.

Jean-Marc Merolla was born in Montbéliard, France, in 1971. He received a Maîtrise de Physique degree from the University of Franche-Comté, Besançon, France, in 1994, and in 1999 a PhD degree in Optical Engineering from the University of Franche-Comté. In 1999, he joined GTL-CNRS Telecom Laboratory in Metz, France, the joint research platform between CNRS and the Georgia Institute of Technology, Atlanta, USA, as a CNRS researcher. Since 2004, he pursues his research activities at the Optics Department of the FEMTO-ST institute in Besançon. His current research includes the study of chaos in optical and electronic systems for secure applications, nonlinear dynamics, quantum optical telecommunication systems, and quantum information processing systems.

John M. Dudley was born in Otahuhu, New Zealand. He received the B.Sc and Ph.D. degrees from the University of Auckland, Auckland, New Zealand, in 1987 and 1992, respectively. During 1992 and 1993, he was a Postdoctoral Researcher at the University of St Andrews, St Andrews, U.K. During 1994, he was a Lecturer at the University of Auckland. Since 2000, he is Professor at the University of Franche-Comté, Besançon, France, where he is currently with the Optics Department, Franche-Comté Electronique Mécanique Thermique et OptiqueSciences et Technologies Institute. He is a member of the Institut Universitaire de France since 2005. Prof. Dudley is currently the Board Chairman of the Quantum Electronics and Optics Division of the European Physical Society. He is an IEEE Lasers and Electro-Optics Society Distinguished Lecturer for the period 20082010. He was elected Fellow of the Optical Society of America in 2007.

Laurent Larger received the Degree in electronic engineering from the University of Paris XI, Orsay, France, in 1988, the Agrégation degree in applied physics in 1991, and the Ph.D. degree in optical engineering and the Habilitation degree from the University of Franche-Comté, Besançon, France, in1997 and 2002, respectively. He was in charge of the International Research Center GTL-CNRS Telecom, a joint laboratory between the French CNRS, Georgia Tech University, Atlanta, and the University of Franche-Comté, Besançon, from 2003 to 2006. He became a Full Professor with the University of Franche-Comté in 2005. He is involved in research with the Franche Comté Electronique, Mécanique Thermique et Optique - Sciences et Technologies Institute, Besançon. His current research interests include the study of chaos in optical and electronic systems for secure communications, delayed nonlinear dynamics, optical telecommunication systems, high spectral purity optoelectronic oscillators, and neuromorphic photonic computing exploiting the complexity of nonlinear dynamical transients. Prof. Larger is a honorary member of the Institut Universitaire de France (nominated as Junior member in 2007). Since January 2012, he is Deputy Director of the FEMTO-ST Research Institute, Besançon.

Christophe Guyeux has taught mathematics and computer science in the Belfort-Montbéliard University Institute of Technologies (IUT-BM) this last decade. He has defended a computer science thesis dealing with security, chaos, and dynamical systems in 2010 under Jacques Bahi's leadership, and is now an associated professor in the computer science department of complex system (DISC), FEMTO-ST Institute, University of Franche-Comté. Since 2010, he has published two books, 9 articles in international journals, and 25 articles in peer reviewed international conferences dealing with security or chaos.

Jacques M. Bahi was born in July, 25th 1961, after a Master of Science in Applied Mathematics, he received a Ph.D in Applied Mathematics from the university of Franche-Comté in 1991. From 1992 to 1999, he was a associate professor of applied mathematics at the Mathematical Laboratory of Besançon, his research interests were focused on parallel synchronous and asynchronous algorithms for differential-algebraic equations and singular systems. Since september 1999, he became a full professor of computer science at the University of Franche-Comté. He published about 150 articles in peer reviewed journal and international conferences and 2 scientific books. Jacques Bahi is a IEEE senior member since 2009. He is the head of the Distributed Numerical Algorithms team of the Computer Science Laboratory of Besançon, he supervised 21 PhD students. He is a member of the editorial board of 2 international journals and is regularly a member of the scientific commitees of many international conferences. Currently, he is interested in 1) high performance computing, 2) distributed numerical algorithms for ad-hoc and sensor networks and 3) dynamical systems with application to data hiding and privacy.