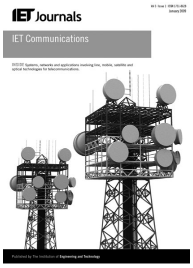
Published in IET Communications
Received on 21st November 2011
Revised on 7th March 2013
Accepted on 15th March 2013
doi: 10.1049/iet-com.2011.0861



ISSN 1751-8628

Randomness of finite-state sequence machine over GF(4) and quality of hopping turbo codes

Luciana De Micco, David Petruzzi, Hilda A. Larrondo, Jorge Castiñeira Moreira

Departamentos de Física y de Ingeniería Electrónica, Facultad de Ingeniera, Universidad Nacional de Mar del Plata. Av. J.B. Justo 4302, 7600 Mar del Plata, Argentina
E-mail: casti@fi.mdp.edu.ar

Abstract: In this study, the authors study a turbo-coding (TC) scheme, whose constituent codes are designed using convolutional encoders. These encoders are finite-state sequence machines (FSSMs) operating over the Galois Field, GF(4). The scheme includes encryption polynomials whose coefficients are selected every L steps, from the set of optimal polynomials of GF(4). Two cases are considered for the polynomial selection: periodical and random. This kind of encoder was studied in a previous study and a correspondence between the randomness of the encoded sequence and performance of the TC was conjectured. The main contribution of this study is to systematically confirm this correspondence, by analysing the randomness of the output and performance of the TC using several randomness quantifiers. Three of the quantifiers are defined on the basis of recurrence plots. Other two quantifiers are defined on the basis of the information theory. All the quantifiers allow one to justify why the proposed TC works better with random selection of the optimal polynomials and with small values of L. In summary, it is shown that a random selection of polynomials and a small L produce FSSMs with enhanced randomness properties and it is also shown that they produce the best quality of the TC, measured by means of the corresponding bit error rate.

1 Introduction

Wireless data networks are specially useful for the transmission of data over very noisy channels. In such environments, the power level of the signal rapidly decays and it could become strongly affected by the noise in the channel. Under these circumstances, the performance of the scheme can be measured by the bit error rate (BER). Additionally, data must be encrypted to provide a security level to the transmission and the strength of the encryption for different attack strategies must be verified. In the design of communication systems for wireless data transmission, it is important the improvement of both the encryption and the error-control coding.

Two main approaches may be used: the traditional approach (TA) is a First-Encrypt-Then-Encode technique. It applies a sequential execution of two separate procedures, first cryptography and then error correcting techniques. Cryptographic algorithms provide security but their decryption counterparts normally need an errorless input for a suitable performance. Furthermore, error-correcting algorithms handle errors in the input data and are not designed to provide security. The other approach, that is the one addressed in this paper, is a crypto-coding-approach (CCA), where encryption and error-correction techniques are performed in a single step [1].

In previous works, [2] it was found that TA is quite efficient, but some degradation is unavoidable, because the encryption itself generates error propagation, specially in those routines of the algorithm devoted to diffusion operations. This issue was analysed in [3, 4] for the particular case of the Advanced Encryption Standard (AES) algorithm. A combination of an encryption algorithm and an efficient error-control code like a low-density parity-check (LDPC) code, diminishes the error propagation effect, but a residual degradation still remains because it is intrinsic to the encryption procedure.

Iterative decoded error-control codes such as LDPC [5] and turbo-coding (TC) [6] may be combined properly with these encryption algorithms to design a communication system with both a good BER performance and security properties. However, if the First-Encrypt-Then-Encode approach is used even in these schemes, a loss in BER performance is unavoidable.

One of the first papers on CCA and the use of error-control coding for encryption purposes is [7]. A different scheme was considered in [8]. In both papers, error-control coding use the non-deterministic polynomial time problem (NP-problem) characteristic of a complex error-control coding scheme, as an encryption technique.

Finite-state sequence machines (FSSMs) were proposed in [6] as constituent encoders of TC. Usually, these FSSMs can operate over a Galois Field, GF(2^n), with $n \geq 1$ a positive integer number. TC that use FSSMs designed over GF(2^n) are suitable to be combined with encryption techniques designed over the same extended field. That is the case of the well-known AES algorithm, that has been designed using operations over GF(2^8). However, for TC using

FSSMs over GF(2^n), decoding complexity increases enormously for $n = 8$.

We consider in this paper a TC scheme whose constituent codes are designed using convolutional encoders with time-varying coefficients. These encoders are FSSMs that operate over the Galois Field, GF(q). The scheme includes an encryption polynomial whose coefficients are changed periodically by means of a user key. The trellis-coding procedure thus hops from one trellis to another, following a random sequence taken over a set of subtrellises which correspond to different convolutional encoders. A trellis-hopping TC using FSSMs defined over finite fields GF (4) was first proposed in [9]. It was conjectured that these FSSMs have a pseudo random output and this randomness produces a trellis-hopping TC with better cryptographic properties tested by means of differential cryptoanalysis [10] and also by brute-force attacks. The proposed schemes have also better BER, showing that encryption and error correction are not in a strong trade-off and consequently, they can be jointly improved. In [11] it was shown that for a given field GF (2^n) there exists a set of several polynomials that are optimal in the sense they produce maximum output sequence length for the all-zero-input.

The main objective in this paper is to systematically study the influence of both, the randomness of the FSSM output and the length L of the trellis-hopping scheme, over the BER of a hopping-TC whose constituent encoders are FSSMs operating over GF(4). The above-mentioned conjecture was tested previously by means of the linear autocorrelation function but conclusive results were not obtained. In this paper randomness of the FSSM output is measured using two kind of quantifiers: information theory quantifiers and recurrence plots (RP) quantifiers. The ability of each quantifier and the coherence between results with different quantifiers, to predict the behaviour of the TC is analysed. Some of these quantifiers have been successfully used in other applications: pseudo random number generators (PRNGs) [12–14], electromagnetic interference improvement [15, 16], distinguishing chaotic and stochastic processes [17], and so on.

To our knowledge this is the first time this issue is systematically studied using statistical tools. We have used a Monte Carlo approach instead of an analytical study because we are interested in a real highly non-linear system and finite length series typical for application purposes. Analytical results are possible only for infinite time series and for quasi-linear systems.

The length of the hopping procedure L, the signal-to-noise ratio, S/N, and both periodic and random hopping are explored. The optimum value of L for cryptographic strength previously determined in [9] is here confirmed but now based on randomness analysis of the FSSM output. The BER of the TC is also evaluated showing that the methodology proposed here also decreases the BER.

The paper is organised in four sections following this introduction. In Section 2, we review the FSSM used as encoder and decoder, and the TC using this FSSM. In Section 3, the new quantifiers considered in this paper are presented. Results for the complete hopping-TC are reported in Section 4. Finally, Section 5 deals with conclusions.

2 FSSM over Galois Fields

Let us first review the FSSM defined over a Galois Field considered in this paper. Fig. 1 shows the block diagram of a FSSM operating as encoder, and its corresponding FSSM decoder. The corresponding 1/2-rate systematic TC is shown in Fig. 2, where the rate 1/2 is obtained by a proper use of puncturing of the outputs of the FSSMs.

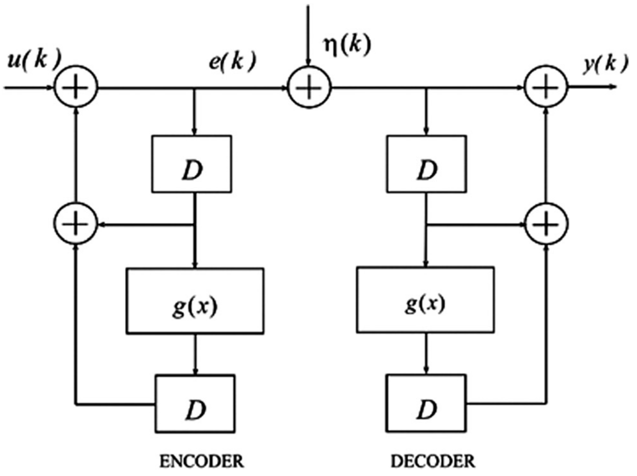


Fig. 1 *FSSM defined over a Galois Field*

As pointed out in [9], a non-systematic structure should be used in order to avoid elementary attacks over the message information. Then, coefficients of the FSSM are changed during transmission every L steps, following a given rule, which can be considered as a user key. This is done in order to increase the privacy levels of the scheme described in Fig. 2.

When a sequence of input values of elements of GF(2^n), $\{u(k)\}$ (see Fig. 1) is an 'all-zero input', the output $\{e(k)\}$ is an oscillating sequence of length l. The selected polynomial in GF(2^n) determines the value of l. Among all possible polynomials in GF(4), those having the form $g(X) = a_0 + a_1 X$, with determined values of coefficients a_0 and a_1 produce the maximum length sequence ($l = L_{\max}$) for the all-zero-input [18]. These are the 'optimal polynomials' as described in Table 1. The value of $L_{\max}$ of an FSSM defined over GF(q) is given by

$$L_{\max} = q^s - 1 \tag{1}$$

where s is the number of states of the FSSM (for GF(4) $L_{\max} = 15$).

In the FSSM studied here, only coefficients of optimal polynomials (see Table 1 for GF(4)) are used. The commuting procedure changes the trellis structure of the coding scheme; that is why the proposed transmission is called 'trellis-hopping TC'.

Two properties are essential for the TC: error correcting ability and cryptographic strength; the first is measured by means of the bit error transmission rate (BER); the second is studied by means of 'differential crypto-analysis' [10] and 'brute-force attack'.

By making a 'differential crypto-analysis' a maximum value of the length of the hop L is determined to be 3 or 4, depending on the structure (non-systematic or systematic) of the trellis-hopping-TC-scheme used [9]. A 'brute-force attack' was also considered in [9]. The number of possibilities over which the eavesdropper should perform this attack for the time-invariant coefficients case is equal to $q^{2(s+m+1)} P_m(NN)$. Here, $P_m(NN)$ is the number of different permutations of the random interleaver and is equal to $NN!$, NN is the size of the interleaver of the TC, s is the number of states of each FSSM, and m is the degree of the

doi: 10.1049/iet-com.2011.0861

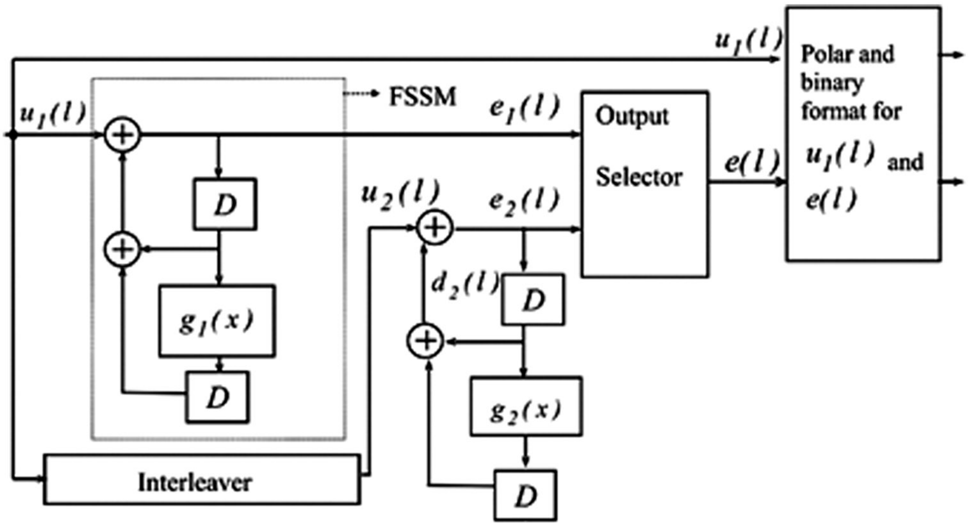


Fig. 2 *Systematic non-linear TC over GF(4)*

Table 1 Optimal polynomials in GF(4)

Galois Field	$g(x)$	Coefficients
GF(4)	$\alpha^p + \alpha X$	$p = 0, 1, 2$
GF(4)	$\alpha^p + \alpha^2 X$	$p = 0, 1, 2$

encryption polynomial $g(x)$. The use of time-varying coefficients increases this amount by the number of hops. Then the number of possibilities over which the eavesdropper should perform the brute-force attack with a hop each L steps is $q^{2(s+m+1)}P_m(NN)((NN)/L)$, [9].

3 Randomness of the FSSM and performance of the TC

Randomness is an extensively studied issue in the context of PRNGs widely used in applications in different fields [19–21]. An ideal PRNG is a 'source of numbers' from a finite 'alphabet' with two basic properties:

- *Equal probability*: all the members of the alphabet must be equally likely, that is the sequence of numbers must have a uniform histogram;
- *Statistical independence*: it is impossible to predict the next value in the sequence as a function of the previous ones.

Equal probability is easier to be tested than statistical independence. In fact, statistical independence can only be proved in a few cases. A useful representation to discover hidden patterns produced by non-linear correlations, and the consequent failure of statistical independence, are two-dimensional and three-dimensional embeddings. Let $\boldsymbol{x}_i$ be an embedding vector with two or three components given by successive values of the time series, tha is: $\boldsymbol{x}_i = (x_i, x_{i+1})$ in the case of a two-dimensional-embedding and $\boldsymbol{x}_i = (x_i, x_{i+1}, x_{i+2})$ in the case of a three-dimensional-embedding. For a random sequence, $\{\boldsymbol{x}_i\}$ must uniformly fill the complete two-dimensional or three-dimensional space meaning that any combination of two or three successive values appears the same number of times. Two- and three-dimensional embeddings allows one to easily discard non-random signals. Unfortunately, to assure statistical independence it is required to extend the procedure to infinite dimensions and this is drawback of visual tools because graphic representations are not possible for dimensions higher than 3.

Different quantifiers were proposed in the literature to define a distance between a given time series and the ideal statistical independence [22–24].

Each quantifier tests the statistical independence from a different point of view and consequently several must be used and all of them must give coherent results.

We study here two groups of quantifiers: the first group is based on the information theory and are referred here as information theory quantifiers; the second group are measures over a RP and are referred here as recurrence plot quantifiers (RPQ).

3.1 Information theory quantifiers

Information theory quantifiers have been successful to classify systems in three categories: deterministic, pseudo-chaotic and stochastic [25]. They are appropriate functionals of the probability distribution function (PDF). Let $\{x_i\}$ be the time series under analysis, with length M. There are infinite possibilities to assign a PDF to a given time series, a subject that will be given because of consideration below. In the meantime, suppose that the PDF is discrete and is given by $\boldsymbol{P} = \{p_i;\ i = 1,\dots, N\}$. Then the normalised Shannon entropy is defined as follows.

Let $S[P]$ be the Shannon entropy

$$S[P] = -\sum_{i=1}^{N} p_i \ln\left(p_i\right) \tag{2}$$

It is well known that the maximum Shannon entropy, $S_{\max} = \ln(N)$, is obtained for a uniform PDF, $\boldsymbol{P}_e = \{1/N,\dots, 1/N\}$. A 'normalised' entropy $H[P]$ can also be defined in the fashion

$$H[P] = S[P]/S_{\max} \tag{3}$$

P itself is not a uniquely defined object and several approaches have been employed in the literature so as to 'extract' P from the given time series. Just to mention some frequently used extraction procedures: (a) time series histogram [26], (b) binary symbolic-dynamics [27], (c) Fourier analysis [28], (d) wavelet transform [29, 30], (e) partition entropies [31], (f) permutation entropy [32, 33], (g) discrete entropies [34], and so on. There is ample liberty to choose among them. De Micco *et al.* [13] proposed two probability distribution as relevant for testing the uniformity of the PDF and the mixing constant: (a) a P based on time series' histograms and (b) a P based on ordinal patterns (permutation ordering) that derives from using the Bandt–Pompe method [35].

For extracting P via the histogram divide the interval [0,1] into a finite number N_{bin} of non-overlapping subintervals A_i: $[0, 1] = \bigcup_{i=1}^{N_{\text{bin}}} A_i$ and $A_i \bigcap A_j = \emptyset \forall i \neq j$. Note that N in (2) is equal to N_{bin}. Of course, in this approach the temporal order of the time-series plays no role at all. The quantifiers obtained via the ensuing PDF are called in this paper H_{hist} and C_{hist}. Let us stress that for time series within a finite alphabet it is relevant to consider an optimal value of N_{bin} (see that is [13]).

For extracting P by recourse to the Bandt–Pompe method the resulting probability distribution P is based on the details of the attractor-reconstruction procedure. 'Causal information' is, consequently, duly incorporated into the construction-process that yields P. The quantifiers obtained via the ensuing PDF are called in this paper H_{BP} and C_{BP}. A notable Bandt–Pompe result consists in getting a clear improvement in the quality of information theory-based quantifiers [12, 14, 17, 25, 36–39].

The extracting procedure is as follows. For the time-series $\{x_t$: $t = 1,\dots, M\}$ and an embedding dimension $D > 1$, one looks for 'ordinal patterns' of order D ([33, 35, 40]) generated by

$$(\boldsymbol{s}) \mapsto \left(x_{s-(D-1)},\ x_{s-(D-2)},\ \dots, x_{s-1},\ x_s\right) \tag{4}$$

which assign to each 'time s' a D-dimensional vector of values pertaining to the times s, $s-1,\dots, s-(D-1)$. Clearly, the greater the D-value, the more information on 'the past' is incorporated into these vectors. By the 'ordinal pattern' related to the time (s) we mean the permutation $\pi = (r_0, r_1,\dots, r_{D-1})$ of $(0, 1,\dots, D-1)$ defined by

$$x_{s-r_{D-1}} \leq x_{s-r_{D-2}} \leq \dots \leq x_{s-r_1} \leq x_{s-r_0} \tag{5}$$

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

$$\boldsymbol{p}(\pi) = \frac{\#\{s|s \leq M - D + 1;\ (s) \quad \text{has type } \pi\}}{M - D + 1} \tag{6}$$

In the last expression the symbol # stands for 'number'.

The advantages of the Bandt–Pompe method reside in (a) its simplicity, (b) the associated extremely fast calculation-process, (c) its robustness in presence of observational and dynamical noise, and (d) its invariance with respect to non-linear monotonous transformations. The Bandt–Pompe's 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 $x_t < x_{t+k}$ should not depend on t [35]. One also assumes that enough data are available for a correct attractor-reconstruction. Of course, the embedding dimension D plays an important role in the evaluation of the appropriate probability distribution because D determines the number of accessible states $D!$. Also, it conditions the minimum acceptable length $M \gg D!$ of the time series that one needs in order to work with a reliable statistics. In relation to this last point Bandt and Pompe suggest, for practical purposes, to work with $3 \leq D \leq 7$ with a time lag $\tau = 1$. This is what we do here (in the present work $D = 6$ is used) [35].

Based on previous works [12–14, 24, 41] we use in this paper two entropies as randomness quantifiers: the normalised permutation entropy H_{BP} [35] and the histogram normalised entropy, H_{hist}. The former detects the presence of ordering patterns in a time series and the latter measures uniformity of the histogram. These patterns represent an unwanted behaviour if statistical independence is required because they are the hallmark of linear or non-linear correlations between consecutive values. For a truly random time series the ideal values are $H_{\text{BP}} = 1$ and $H_{\text{hist}} = 1$.

3.2 Quantifiers based on RP

RP were introduced by Eckmann *et al.* [42] so as to visualise the recurrence of states during phase space-evolution. The RP is a two-dimensional representation in which axes x and y are both time-axes. The recurrence or not of a state at two given times t_i, t_j is pictured in this graph by means of either black or white dots, where a black dot signals a recurrence. Of course only periodic continuous systems have exact recurrences. In discrete systems one detects only approximate recurrences, up to an error ε. The so-called recurrence function is defined as follows

$$\boldsymbol{R}_{ij}(\varepsilon) = \Theta\left(\varepsilon - \|\boldsymbol{x}(i) - \boldsymbol{x}(j)\|\right) \tag{7}$$

with $\boldsymbol{R}_{ij}(\varepsilon)$ and $\boldsymbol{x}(i) \in \Re$, belong to the set of real numbers, and $i, j = 1,\dots, N$. Being N the number of discrete states $\boldsymbol{x}(i)$ considered, $\|.\|$ is a norm, and $\Theta(.)$ is the Heaviside step function, [35].

In the particular case analysed in this paper, $\{e(k)\}$ is a one-dimensional series but the recurrence function-idea can be extended to D-dimensional phase spaces or even to suitably reconstructed embedding phase spaces. Of course, the visual impact produced by the RP is insufficient to compare the quality of different random sequences, because of the 'small scale' structures that may be present. Several measures have been defined to quantify these small scale structures [22], each measure being a functional of $\boldsymbol{R}_{ij}(\varepsilon)$ (7). In this paper, three RPQ are considered:

1. *The recurrence rate (RR)*, given by

$$\text{RR}(\varepsilon) = \frac{1}{N^2} \sum_{i,j=1}^{N} \boldsymbol{R}_{ij}(\varepsilon) \tag{8}$$

This is a measure based on the RP density. In the limit $N \to \infty$, RR is the probability that a state recurs to its ε-neighbourhood in phase space. For random series the ideal value would be $\text{RR} = 0$. However, in practice, the zero value is never obtained because if no points are found in the RP, a larger ε is adopted in order that the quantifiers may make sense.

2. *Two diagonal measures*: they are measures related to the histogram $P(\varepsilon, l)$ of diagonal line lengths (l), given by

$$P(\varepsilon,\ l) = \sum_{i,j=1}^{N} \Big[1 - \boldsymbol{R}_{i-1,\,j-1}(\varepsilon)\Big]\Big[1 - \boldsymbol{R}_{i+l,\,j+l}(\varepsilon)\Big] \times \prod_{k=0}^{l-1} \boldsymbol{R}_{i+k,\,j+k}(\varepsilon) \qquad (9)$$

Processes with uncorrelated or weakly correlated behaviour originate no (or just very short) diagonals, whereas deterministic processes give rise to 'long' diagonals and smaller amount of single, isolated RPs. The measures considered here are:

(a) The average diagonal line length L_{diag}

$$L_{\text{diag}} = \frac{\sum_{l=l_{\min}}^{N} lP(\varepsilon,\ l)}{\sum_{l=l_{\min}}^{N} P(\varepsilon,\ l)} \qquad (10)$$

$l_{\min}$ is the minimum length of diagonal lines. Here, we consider $l_{\min} = 2$; $\varepsilon = 0.1$. The randomness increases as L_{diag} diminishes because smaller values of L_{diag} imply long time statistical independence.

(b) The entropy of the distribution $P(\varepsilon,\ l)$ is denoted as ENTR and is given by:

$$\text{ENTR} = -\sum_{l=l_{\min}}^{N} P(\varepsilon,\ l) \ln P(\varepsilon,\ l) \qquad (11)$$

Randomness does not require a high value of ENTR because ENTR measures the histogram of diagonal lines and a high value means all lengths of diagonal lines are present. In fact the best situation for randomness is to have only very short diagonal lines and consequently the histogram of diagonal lines will have a delta-like aspect and a small value of ENTR will be obtained. On the contrary a small value of ENTR with large values of L_{diag} implies that only long diagonal lines are present. This is an unwanted behaviour in a random time series. Consequently, the value of ENTR must be considered in conjunction with the value of L_{diag}.

4 Results

The aim of this work is to systematically test the relation between the randomness of the output of the FSSM $\{e(k)\}$ (see Fig. 1) and the performance of the proposed TC for which the FSSM is its constituent encoder. Consequently, we need to measure the randomness of the output $\{e(k)\}$ of the FSSM of Fig. 1 and also the BER of the TC. The analysis must be made for different S/N.

We have studied two options for the hopping procedure: (a) periodic hopping, that is the first polynomial is used during L steps, then the second polynomial, and so on. With this procedure all the optimal polynomial are used in the process and always in the same order. (b) random hopping, that is the order of the polynomials is selected 'at chance' by means of a random variable. The 'no-hopping' scheme was also evaluated for comparison.

In the evaluation of periodic hopping 720 realisations of a time series $\{e(k)\}$ with 16 000 values each, were evaluated for L, because there are 720 possible orderings of the six optimal polynomials. In the evaluation of random hopping 100 realisations of a time series $\{e(k)\}$ with 16 000 values each were analysed for $L = 1, 2, 4, 8, 16$. In the no-hopping scheme six realisations were analysed, one for each optimal polynomial. In all cases, H_{BP} and H_{hist} were evaluated with an embedding dimension $D = 6$. For every L the mean value $\langle H_{\text{BP}} \rangle$, $\langle H_{\text{hist}} \rangle$ and the standard deviation σ_H over the realisations were determined. With the number of realisations used for each case $\sigma_H / \langle H \rangle \leq 0.05$.

4.1 Randomness of {e(k)}

Results are shown in Figs. 3 and 4, where the randomness of $\{e(k)\}$ for periodic hopping (Fig. 3) and random hopping (Fig. 4) are compared with the no-hopping case.

The analysis of Fig. 3 shows that for periodic hopping:

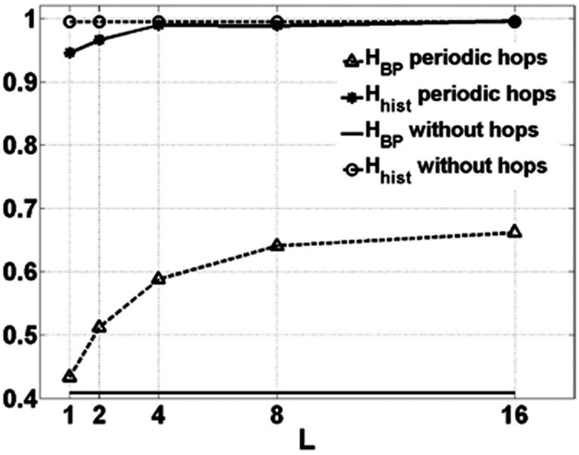


Fig. 3 *Mean value over 720 realisations of the permutation entropy H_{BP} and H_{hist} as a function of L for periodic hopping between the optimal polynomials of GF(4)*

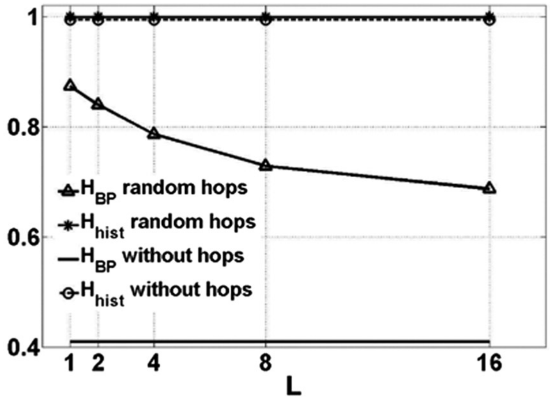


Fig. 4 *Mean value over 100 realisations of the permutation entropy H_{BP} and H_{hist} as a function of L for random hopping between the optimal polynomials of GF(4)*

- H_{hist} decreases a little with the hopping procedure. This is an unwanted behaviour because it means that $\{e(k)\}$ has a less uniform histogram. The situation is worse with small values of L.
- H_{BP} is extremely low without hopping, showing that some ordering patterns in $\{e(k)\}$ are more frequent than others. Periodic hopping improves ordering patterns distribution, as it is shown by the increase in H_{BP}. However, $H_{\text{BP}} \cong 0.4$ still a very low value.
- The best values of both H_{BP} and H_{hist} are obtained for $L=16$, a non-recommended value from cryptanalysis point of view [9].

The conclusion of Fig. 3 is periodic hopping lightly improve the randomness of $\{e(k)\}$ for high values of L.

The analysis of Fig. 4 shows that for random hopping:

- H_{hist} increases a little with the hopping procedure and remains almost equal to the ideal value $H_{\text{hist}}=1$ in spite of the value of L.
- H_{BP} decreases as L incresases and it has a value considerable higher as compared with its value without hops.
- The best values of both H_{BP} and H_{hist} are obtained for $L=1$, a recommended value from cryptanalysis point of view.

The conclusion of Fig. 4 is random hopping highly improve the randomness of $\{e(k)\}$ specially for small values of L.

In Figs. 5 and 6 the RP quantifiers RR, L_{diag} and ENTR are shown for periodic and random-hopping procedures, respectively. In order to show all of them in the same plot each quantifier has been normalised as follows

$$\widetilde{x} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{12}$$

where x runs for L_{diag} or RR or ENTR, respectively. The case without hopping produces values for L_{diag}, RR and ENTR very far from the values for the cases with hopping. That is the reason they are not represented in the same plot. These values are: $L_{\text{diag}}=3995$, $\text{RR}=0.253$ and $\text{ENTR}=6.27$ (as mentioned in the captions of Figs. 5 and 6).

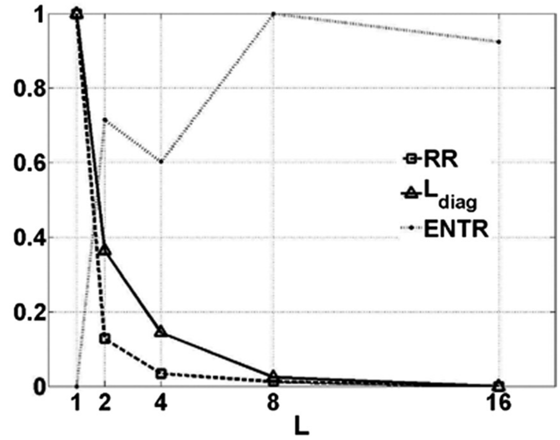


Fig. 5 *Normalised mean value over 10 realisations of the RP quantifiers as a function of L for periodic hopping between the optimal polynomials of GF(4)*

Without hopping the corresponding values are $L_{\text{diag}}=3995$, $\text{RR}=0.253$ and $\text{ENTR}=6.27$

Normalisation constants are (see (12)): $L_{\text{diag}}^{\min}=2.4107$, $L_{\text{diag}}^{\max}=2.4148$, $RR^{\min}=0.25001$, $RR^{\max}=0.25003$, $\text{ENTR}^{\min}=0.6245$, $\text{ENTR}^{\max}=0.8527$

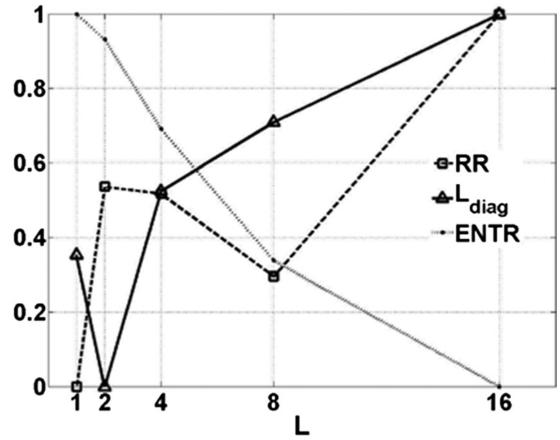


Fig. 6 *Normalised value over 10 realisations of the RP quantifiers as a function of L for random hopping between the optimal polynomials of GF(4)*

Without hopping the corresponding values are $L_{\text{diag}}=3995$, $\text{RR}=0.253$ and $\text{ENTR}=6.27$

Normalisation constants are (see (12)): $L_{\text{diag}}^{\min}=2.4107$, $L_{\text{diag}}^{\max}=2.4148$, $\text{RR}^{\min}=0.25001$, $\text{RR}^{\max}=0.25003$, $\text{ENTR}^{\min}=0.6245$, $\text{ENTR}^{\max}=0.8527$

The analysis of Fig. 5 shows that for periodic hopping:

- *RR* decreases as L increases and the smallest values are obtained for $L=16$, a non-recommended value from cryptanalysis point of view.
- L_{diag} also decreases as L increases and the smallest value is obtained for $L=16$.
- ENTR increases with L. It means that, despite of the fluctuations of ENTR, in the area of our interest (small values of L) many diagonal lines with a large L_{diag} are obtained in the RP, this is not a desirable behaviour.

The conclusion of Fig. 5 is again that periodic-hopping sequence $\{e(k)\}$ have bad statistical properties measured by RP quantifiers (in spite they are much better than the statistical properties of $\{e(k)\}$ without hopping).

The analysis of Fig. 6 shows that for random hopping:

- RR is minimum for $L=1$ and maximum for $L=16$.
- L_{diag} increases as L increases and the smallest value is obtained for $L=2$.
- ENTR decreases as L increases. It means that for small values of L, diagonal lines of various lengths can be seen in the RP.

In the random hopping case RR and $L_{\min}$ both quantifiers show that for large values of L the sequences present more correlations. The conclusion of Fig. 6 is random-hopping sequence $\{e(k)\}$ have the best statistical properties for small values of L. It is much better than $\{e(k)\}$ without hopping as measured by RP.

4.2 Error correction performance of the TC

In order to test the quality of the TC the BER of the whole system was evaluated by means of a Monte Carlo simulation involving the transmission of 10 rounds of 50 000 blocks of length 400 symbols each, for every choice in L. In GF(4) there exist six different optimal polynomials (see Table 1) and each element $\{e(k)\}$ is in the set $\{0, 1, \alpha, \alpha^2\}$. We are specially interested in determining the BER performance of the scheme for small values of L, in view of crypto-analysis and brut-force-attack-analysis previously done [9].

The TC has a block interleaver of size 400. Additive white Gaussian noise (AWGN) was added in the channel with different S/N ratios. Decoding was performed using the LogMap/BCJR algorithm [43] with 15 iterations.

Results are shown in Figs. 7–9 where the mean values over all the rounds are depicted as functions of S/N and L. The number of realisations guarantee $\sigma_{\mathrm{BER}}/ \leq 0.05$ in all cases.

Fig. 7 shows that the trellis-hopping procedure with small values of L and random hopping, results into an improvement in the BER performance over that obtained with the non-hopping case. Note that the small values of L are precisely those producing maximum randomness of $\{e(k)\}$ as measured by means of all the considered randomness quantifiers (see Section 4.1).

Fig. 8 compares the BER performance as a function of S/N for the no-hopping TC scheme and for periodic and random hopping of the polynomials every $L = 4$ steps. It is clear that the best results are obtained with the random hopping choice [9]. For $L \geq 4$ any hopping procedure works fine but these large values of L are not adequate for cryptographic strength.

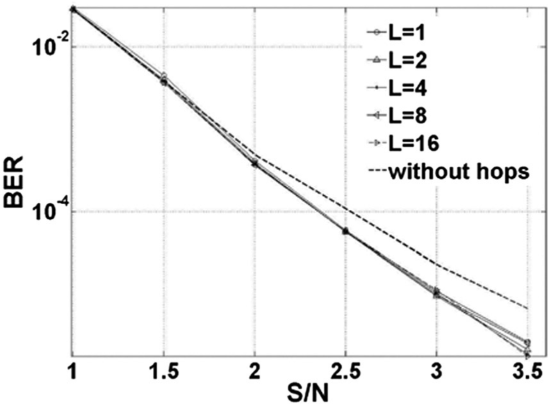


Fig. 7 *Mean value of BER as a function of S/N for random hopping between the optimal polynomials of GF(4), for different values of the hopping length L*

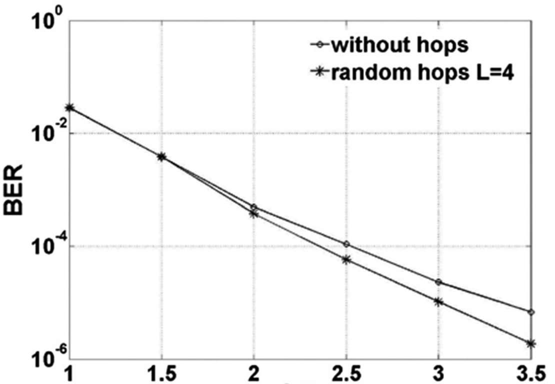


Fig. 8 *Mean value of BER as a function of S/N for periodic and random hopping between the optimal polynomials of GF(4), with L = 4*

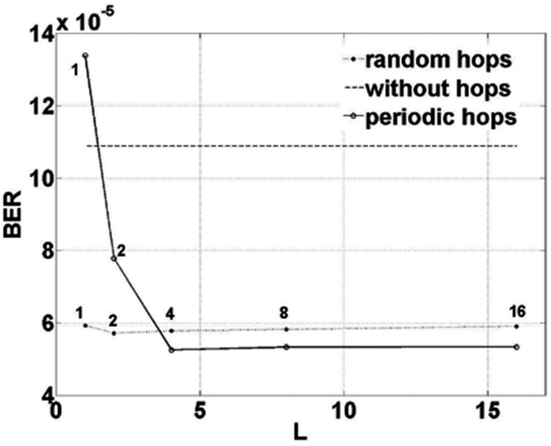


Fig. 9 *Mean value of BER as a function of L for periodic and random hopping between the optimal polynomials of GF(4), with S/N = 2.5*

Fig. 8 compares the BER performances for S/N = 2.5 with periodic-hopping, random-hopping and no-hopping schemes. Note that for this low vaue of L the best performance is obtained with the random-hopping option.

5 Conclusions

In summary, in the present work we have made a systematic analysis of how the randomness of $\{e(k)\}$, the FSSM output, is related to the BER performance of the TC. We can summarise the main results as follows:

- We have verified the correspondence between the BER performance of the trellis-hopping scheme and the randomness of the output $\{e(k)\}$ of the FSSM (presented as a conjecture in previous works [9]).
- BER has been studied by means of a Monte Carlo procedure and extensive simulations, not only as a function of S/N but also as a function of L.
- Five randomness quantifiers, two of them from the information theory and three of them from the Rps theory, successfully detect the randomness of $\{e(k)\}$.
- Both (periodic and random) hopping procedures increase randomness of $\{e(k)\}$ and also the BER of theTC when compared with those obtained for the no-hopping scheme.
- For small values of L ($L \leq 4$) and a reasonable value of S/N, $2 \lesssim \mathrm{S/N} \lesssim 3$ random-hopping produces the best results.
- For higher values of L ($L \geq 4$) random- and periodic-hopping produce similar results. However, large values of L are not recommended for cryptographic strength.

The main conclusion is that the proposed random-hopping TC can improve both security and reliability of the transmission. The use of chaotic sources instead of random ones in both the hopping procedure and the interleaver is under study and will be published elsewhere.

6 Acknowledgments

Luciana De Micco, Hilda A. Larrondo and Jorge Castineira are researchers of Consejo Nacional de Investigaciones Cientficas y Técnicas (CONICET). This work was partially supported by ANPCyT (PIP 112-200801-01420) and UNMDP Argentina.

7 References

1 Mathur, C.N.: ‘A mathematical framework for combining error correction and encryption’. PhD dissertation, Stevens Institute of Technology, Castle Point on Hudson, 2007

2 Arnone, L., González, C., Gayoso, C., Castiñeira Moreira, J., Liberatori, M.C.: ‘Security and BER performance trade-off in wireless communication systems applications’, *Latin Am. Appl. Res.*, 1978, **39**, pp. 187–192

3 Coppolillo, L., Liberatori, M.C., Petruzzi, D.M., Castiñeira Moreira, J.: ‘Analysis of error propagation of AES encrypted information transmission in noisy channels’. Proc. RPIC XIII, 2009

4 Coppolillo, L., Liberatori, M.C., Petruzzi, J.C., Bonadero D.M., Castińeira Moreira, J.: ‘Characteristics of AES encrypted data transmission in noisy channels as a measure of the AES algorithm encryption capability’. Proc. of AST 2009, **2009**, pp. 250–264.

5 MacKay, D.J.C., Neal, R.M.: ‘Near Shannon limit performance of low density parity-check codes’, *Electron. Lett.*, 1997, **3**, (6), pp. 457–458

6 Berrou, C., Glavieux, A., Thitimajshima, P.: ‘Near Shannon limit error-correcting coding and decoding: turbo codes’. Proc. 1993 IEEE Int. Conf. Communications, 1993

7 McEliece, R.J.: ‘A public-key cryptosystem based on algebraic coding theory’. DSN Progress Report, 1978

8 Niederreiter, H.: ‘Knapsack-type cryptosystems and algebraic coding theory’, *Probl. Control Inf. Theory*, 1986, **15**, (2), pp. 157–166

9 Liberatori, M.C., Castieira Moreira, J., Petruzzi, D.M., Honary, B.: ‘Trellis-hopping turbo coding’, *IEE Proc.-Commun*., 2006, **153**, (6), pp. 966–975

10 Chambers, W.G.: ‘Comment to chaotic digital encoding: An approach to secure communication’, *IEEE Trans. Circuits Syst. II*, 1999, **46**, (11), pp. 1445–1447

11 Petruzzi, D.M., Castiñeira Moreira, J., Levin, D.G.: ‘Quasi chaotic coding over GF(q)’, *IEEE Trans. Commun.*, 2006, **54**, (3), pp. 462–468

12 Larrondo, H.A., Martín, M.T., González, C.M., Plastino, A., Rosso, O. A.: ‘Random number generators and causality’, *Phys. Lett. A*, 2006, **352**, (4–5), pp. 421–425

13 De Micco, L., González, C.M., Larrondo, H.A., Martín, M.T., Plastino, A., Rosso, O.A.: ‘Randomizing nonlinear maps via symbolic dynamics’, *Physica A*, 2008, **387**, pp. 3373–3383

14 Larrondo, H.A., González, C.M., Martín, M.T., Plastino, A., Rosso, O. A.: ‘Intensive statistical complexity measure of pseudorandom number generators’, *Physica A*, 2005, **356**, pp. 133–138

15 De Micco, L., Petrocelli, R.A., Rosso, O.A., Plastino, A., Larrondo, H. A.: ‘Mixing chaotic maps and electromagnetic interference reduction’, *IJAMAS Special Issue (SI)*‘ *Stat. Chaos Complexit*’, 2012, **26**, (2), pp. 105–120

16 Callegari, S., Rovatti, R., Setti, G.: ‘Chaotic modulations can outperform random ones in electromagnetic interference reduction tasks’, *Electron. Lett.*, 2002, **38**, (12), pp. 543–544

17 Rosso, O.A., Larrondo, H.A., Martín, M.T., Plastino, A., Fuentes, M.A.: ‘Distinguishing noise from chaos’, *Phys. Rev. Lett*., 2007, **99**, pp. 154102–154106

18 Liberatori, M.C., Petruzzi, D.M., Castiñeira Moreira, J., Bonadero, J.C.: ‘Exit chart analysis of nonlinear turbo coding over GF(4)’, *IET Commun*., 2008, **2**, (5), pp. 630–641

19 L’Ecuyer, P.: ‘Uniform random number generation’, *Ann. Oper. Res.*, 1994, **53**, pp. 77–120

20 Haar, M.: ‘A lot of stuff concerning random numbers, available online. http://www.random.org/randomness/, 1997

21 Gammel, B.M.: ‘Hurst’s rescaled range statistical analysis for pseudorandom number generators used in physical simulations’, *Phys. Rev. E*, 1998, **58**, (2), pp. 2586–2597

22 Marwan, N., Romano, M.C., Thiel, M., Kurths, J.: ‘Recurrence plots for the analysis of complex systems’, *Phys. Rep.*, 2007, **438**, pp. 237–329

23 Feldman, D.P., McTague, C.S., Crutchfield, P.: ‘The organization of intrinsic computation: complexity-entropy diagrams and the diversity of natural information processing’, *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2008, **18**, (4), p. 43106

24 De Micco, L., Larrondo, H.A., Plastino, A., Rosso, O.A.: ‘Quantifiers for randomness of chaotic pseudo random number generators’, *Philos. Trans. R. Soc. A*, 2009, **367**, pp. 3281–3296

25 Rosso, O.A., Zunino, L., Pérez, D.G., *et al*.: ‘Extracting features of Gaussian selfsimilar stochastic processes via the Bandt & Pompe approach’, *Phys. Rev. E*, 2007, **76**, (6), p. 061114

26 Martin, M.T.: ‘Transformada Wavelet y Teoría de información en el análisis de señales complejas’. PhD 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**, pp. 1114–1147

28 Powell, G.E., Percival, I.C.: ‘A spectral entropy method for distinguishing regular and irregular motion of Hamiltonian systems’, *J. Phys. A: Math. Gen*., 1979, **12**, pp. 2053–2071

29 Blanco, S., Figliola, A., Quian Quiroga, R., Rosso, O.A., Serrano, E.: ‘Time-frequency analysis of electroencephalogram series (iii): wavelet packets and information cost function’, *Phys. Rev. E*, 1998, **57**, pp. 932–940

30 Rosso, O.A., Blanco, S., Jordanova, J., *et al*.: ‘Wavelet entropy: a new tool for analysis of short duration brain electrical signals’, *J. Neurosci. Methods*, 2001, **105**, pp. 65–75

31 Ebeling, W., Steuer, R.: ‘Partition-based entropies of deterministic and stochastic maps’, *Stoch. Dyn.*, 2001, **1**, (1), pp. 1–17

32 Bandt, C., Keller, G., Pompe, B.: ‘Entropy of interval maps via permutations’. *Nonlinearity*, 2002, **15**, pp. 1595–1602

33 Keller, K., Sinn, M.: ‘Ordinal analysis of time series’, *Physica A*, 2005, **356**, pp. 114–120

34 Amigó, J.M., Kocarev, L., Tomovski, I.: ‘Discrete entropy’, *Physica D*, 2007, **228**, pp. 77–85

35 Bandt, C., Pompe, B.: ‘Permutation entropy: a natural complexity measure for time series’, *Phys. Rev. Lett*., 2002, **88**, pp. 174102–1

36 Kowalski, A.M., Martín, M.T., Plastino, A., Rosso, O.A.: ‘Bandt–Pompe approach to the classical-quantum transition’, *Physica D*, 2007, **233**, pp. 21–31

37 Rosso, O.A., Vicente, R., Mirasso, C.R.: ‘Encryption test of pseudo-aleatory messages embedded on chaotic laser signals: an information theory approach’, *Phys. Lett. A*, 2008, **372**, pp. 1018–1023

38 Zunino, L., Pérez, D.G., Martín, M.T., Plastino, A., Garavaglia, M., Rosso, O.A.: ‘Characterization of Gaussian self-similar stochastic processes using wavelet-based informational tools’, *Phys. Rev. E*, 2007, **75**, pp. 021115

39 Zunino, L., Pérez, D.G., Martín, M.T., Garavaglia, M., Plastino, A., Rosso, O.A.: ‘Permutation entropy of fractional Brownian motion and fractional Gaussian noise’, *Phys. Lett. A*, 2008, **372**, (27–28), pp. 4768–4774

40 Keller, K., Lauffer, H.: ‘Symbolic analysis of high-dimensional time series’, *Int. J. Bifurcation Chaos*, 2003, **13**, pp. 2657–2668

41 González, C.M., Larrondo, H.A., Rosso, O.A.: ‘Statistical complexity measure of pseudorandom bit generators’, *Physica A*, 2005, **354**, pp. 281–300

42 Eckmann, J., Oliffson Kamphorst, S., Ruelle, D.: ‘Recurrence plots of dynamical systems’, *Europhys. Lett*., 1987, **4**, pp. 973–977

43 Robertson, P., Hoeher, P., Villebrun, E.: ‘Optimal and sub-optimal maximum a posteriori algorithms suitable for turbo decoding’, *Eur. Trans. Telecommun.*, 1997, **8**, pp. 119–125