

Design and Analyses of some 1-D Chaotic Generators for Secure Data

Safwan EL ASSAD^{*}, Hassan NOURA^{*}, Qianxue WANG^{*}, Ina TARALOVA^{**}

^{*}*IRRENA: Institut de Recherche en électronique et Electrotechnique de Nantes Atlantique
Polytech'Nantes, Rue Christian pauc BP 50609 Nantes Cedex 3, France*

safwan.elassad@univ-nantes.fr

hassan.noura@univ-nantes.fr

qianxue.wang@etu.univ-nantes.fr

^{**}*IRCCyN: Institut de recherche en communications et Cybernétique de Nantes*

Ina.Taralova@ircryn.ec-nantes.fr

Abstract: In this paper, we study, design, and implement under Matlab/Simulink some 1-D digital chaos generation methods to secure data. All designed generators have the same structure, but using two different non-linear functions (left circulate function LCIRC, $L_n x$) and containing one or two cascading stages. We display the importance of the perturbing orbit technique and the cascading technique, to avoid the dynamical degradation caused by 2^N -dimensional finite space states. The first technique increases also the orbit cycle length. Finally, to quantify the security level, we perform a comparative study of the dynamical statistical properties: noise-like autocorrelation, cross-correlation, uniformity, attractors, and NIST (National Institute of Standards and Technology) tests obtained under simulation.

Key words: Chaotic generators, perturbed technique, cascaded technique, NIST tests.

INTRODUCTION

In today's highly computerized and interconnected world, interest has been growing in the use of chaos for secure communications, and the idea of using digital chaotic systems to construct cryptography and pseudo-random coding has been extensively studied since 1990s. The security of the transmitted information through a channel, against passive or active attacks is an international concern. The use of the chaotic signals to mask useful information and to make it unrecognizable (by modulation or encryption) by an intruder is a field of research in full expansion. So, we need a digital chaotic signal with good cryptographic properties, such as: balance on $\{0, 1\}$; long cycle-length; δ -like autocorrelation; cross-correlation near to zero; desired attractor; and having good tests NIST.

To obtain better dynamical statistical properties and avoid the dynamical degradation caused by the digital chaotic systems working in a 2^N -dimensional finite space, three techniques can be used: adding more delays, cascading multiple chaotic systems and

perturbing chaotic orbit. All these techniques are implemented and tested.

In this paper, we improve the Frey map, by including a pseudo randomly perturbing technique of the chaotic orbit and we study some new systems to generate chaotic signals with desired statistical properties.

After, we perform a comparative analysis of obtained simulation results of the dynamical signal properties before concluding.

1. Perturbed chaotic orbit technique

To improve the dynamical signal properties, a perturbation based algorithm is used. Indeed, the cycle length is expanded and good statistical properties are reached [Tao 2001], [El Assad 2008].

Considering a one dimensional chaotic generator defined by:

$$x(n) = F[x(n-1)] \in [0,1] \quad x(n) \in [0,1] \quad n=1,2,\dots \quad (1)$$

Here, for computing precision N , each x can be described:

$$x(n) = 0, x_1(n)x_2(n)\dots x_i(n)\dots x_N(n) \quad x_i(n) \in \{0,1\} \quad (2)$$

$$i = 1, 2, \dots, N$$

The fundamental basis of the perturbing method is the fact that no stable cycles exist, i.e. the chaotic system having entered a cycle can be driven to leave the cycle immediately by a perturbation, and will run away from the cycle after iterations. The choice of the perturbation is done according to the following principles: it should have controllable long cycle length and uniform distribution; it should not degrade the good statistical properties of chaos dynamics, so the magnitude of the perturbing signal must be much smaller than that of the chaotic signal. The signal-to-noise ratio is defined as:

$$SNR = 10 \times \log\left(\frac{\text{maximum magnitude of chaotic signal}}{\text{maximum magnitude of perturbing signal}}\right) \quad (3)$$

A suitable candidate for the perturbing signal generator is the maximal length LFSR because its generated sequences have the following advantages: 1) definite cycle length ($2^k - 1$) (k is the degree); 2) uniform distribution; 3) delta like autocorrelation function; 4) easy implementation; 5) controllable maximum signal magnitude given by $2^N \times (2^k - 1)$ when used in N -precision system.

The perturbing bit for every n clock time can be generated as following:

$$Q_{k-1}^+(n) = Q_k(n) = g_0 Q_0(n) \oplus g_1 Q_1(n) \oplus \dots \oplus g_{k-1} Q_{k-1}(n) \quad (4)$$

$$\text{with } n = 0, 1, 2, \dots$$

Where \oplus represents 'exclusive or', $g_0 g_1 \dots g_{k-1}$ are the tap coefficients of the primitive polynomial generator, and $Q_0 Q_1 \dots Q_{k-1}$ are the initial register values of which at least one is non zero. The perturbation starts at $n = 0$, and the next ones occur periodically every Δ iterations (Δ is a positive integer), with $n = l \times \Delta$, $l = 1, 2, \dots$. The perturbed sequence is given by the equation (5):

$$x_i(n) = \begin{cases} F[x_i(n-1)] & 1 \leq i \leq N-k \\ F[x_i(n-1)] \oplus Q_{N-i}(n) & N-k+1 \leq i \leq N \end{cases} \quad (5)$$

Where $F[x_i(n)]$ represents the i th bit of $F[x(n)]$.

The perturbation is applied on the last k bits of $F[x(n)]$. When $n \neq l \times \Delta$, no perturbation occurs, and then $x(n) = F[x(n-1)]$.

The system cycle length is given by the following relation (see appendix):

$$T = \sigma \times \Delta \times (2^k - 1) \quad (6)$$

Where σ is a positive integer. The lower bound of the system cycle length is:

$$T_{\min} = \Delta \times (2^k - 1) \quad (7)$$

2. Presentation of developed techniques

2.1. Frey map

An approach to generate chaos for secure communications has been demonstrated by Frey. The codec uses a non linear filter with finite precision (N bits) in conjunction with its inverse filter. The non linear function used is the left circulate function suited to hardware implementation. The general equation of Frey generator is defined by the following relation [Frey 1993], [El Assad 2006]:

$$e_u(n) = F_{NL}\{k_u(n) + \sum_{i=1}^m [G_i \times e_u(n-D_i) + s(n)]\} \quad (8)$$

The u index in equation (8) denotes an unsigned number. Also, all additions are modulo 2^N . These operators are assumed to be generally nonlinear operations.

The generator scheme consists in a non linear function $F_{NL}(x)$ with a delayed feedback loop.

A particular case (3 delays) of the system driven by equation (8), is shown in figure 1. All operations inside the loop work in the unsigned number representation modulo 2^N . The delivered chaotic signal $e_u(n)$ is composed by 2^N quantized levels including the interval between $[0, 2^N - 1]$, and having the duration of T_{ch} seconds for each chip:

$$e_u(n) = \text{mod}\{k_u(n) + \text{mod}\{x_1(n) + \text{mod}[x_2(n) + x_3(n)]\}\} \\ e_u(n) = \text{mod}[k_u(n) + x_1(n) + x_2(n) + x_3(n)] \quad (9)$$

$$x_1(n) = e_u(n-1) \\ x_2(n) = e_u(n-2) \\ x_3(n) = \text{lcirc}[e_u(n-3)] = \text{mod}[2e_u(n-3) + s_u(n-1)] \quad (10)$$

$$s(n-1) = \begin{cases} 0 & \text{if } e_u(n-3) < 2^{N-1} \\ 1 & \text{otherwise} \end{cases} \quad (11)$$

Where N is the binary word length, and x_1, x_2 and x_3 are the states, namely, the outputs of the delays. Combining these equations, we obtain:

$$e_u(n) = \text{mod}[k_u(n) + e_u(n-1) + e_u(n-2) + 2e_u(n-3) + s_u(n-1)] \quad (12)$$

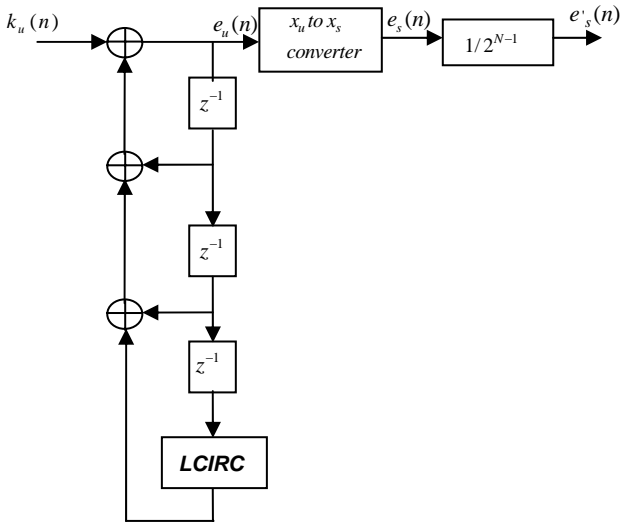


Figure 1: Frey structure generator under test

The input signal $k_u(n)$ plays in our application the role of an additional key, which does not allow an unauthorized eavesdropper to recover the generated signal. However $k_u(n)$ can be used as information signal to encrypt.

In order to reduce the signal's mean power, and to make its amplitude independent of the number of levels (in fact, on N), the generated signal $e_u(n)$ is, first converted into a signed signal $e_s(n)$ (The index s means «signed») in the 2 's complement in the 2^N representation set, $[C2, 2^N]$, and then normalized by the maximum absolute value of the quantized levels. Hence, the effective generated signal is: $e'_s(n) = \sum_n q_n \times p_{T_{ch}}(t - nT_{ch})$ with :

$$\frac{-2^{N-1}}{2^{N-1}} \leq q_n < \frac{2^{N-1}-1}{2^{N-1}} \Leftrightarrow -1 \leq q_n < 1$$

and

$$p_{T_{ch}} = \begin{cases} 1 & \text{if } 0 \leq t < T_{ch} \\ 0 & \text{otherwise} \end{cases}$$

2.2. Two Cascaded Frey map

Cascading two chaotic systems will let the output of the generator be more complex [TAN 04], [WAN 08]. The equations of two cascaded Frey map are written as follows (see figure2):

$$e_{u1}(n) = \text{mod}\{k_u(n) + \text{mod}\{x_{11}(n) + \text{mod}[x_{12}(n) + x_{13}(n)]\}\} \quad (13)$$

$$e_{u1}(n) = \text{mod}[k_u(n) + x_{11}(n) + x_{12}(n) + x_{13}(n)]$$

$$e_{u2}(n) = \text{mod}\{e_{u1}(n) + \text{mod}\{x_{21}(n) + \text{mod}[x_{22}(n) + x_{23}(n)]\}\}$$

$$e_{u2}(n) = \text{mod}[e_{u1}(n) + x_{21}(n) + x_{22}(n) + x_{23}(n)] \quad (14)$$

$$\begin{aligned} x_{11}(n) &= e_{u1}(n-1) \\ x_{12}(n) &= e_{u1}(n-2) \\ x_{13}(n) &= \text{lcirc}[e_{u1}(n-3)] = \\ &\quad \text{mod}[2e_{u1}(n-3) + s_{u1}(n-1)] \end{aligned}$$

$$x_{21}(n) = e_{u2}(n-1) \quad (15)$$

$$x_{22}(n) = e_{u2}(n-2)$$

$$x_{23}(n) = \text{lcirc}[e_{u2}(n-3)] = \text{mod}[2e_{u2}(n-3) + s_{u2}(n-1)] \quad (16)$$

$$s(n-1) = \begin{cases} 0 & \text{if } e_u(n-3) < 2^{N-1} \\ 1 & \text{otherwise} \end{cases} \quad (17)$$

By combining the above equations, we obtain:

$$\begin{aligned} e_{u1}(n) &= \text{mod}[k_u(n) + e_{u1}(n-1) + e_{u1}(n-2) + 2e_{u1}(n-3) + s_{u1}(n-1)] \\ e_{u2}(n) &= \text{mod}[k_u(n) + e_{u1}(n-1) + e_{u1}(n-2) + 2e_{u1}(n-3) + \\ &\quad s_{u1}(n-1) + e_{u2}(n-1) + e_{u2}(n-2) + 2e_{u2}(n-3) + s_{u2}(n-1)] \end{aligned} \quad (18)$$

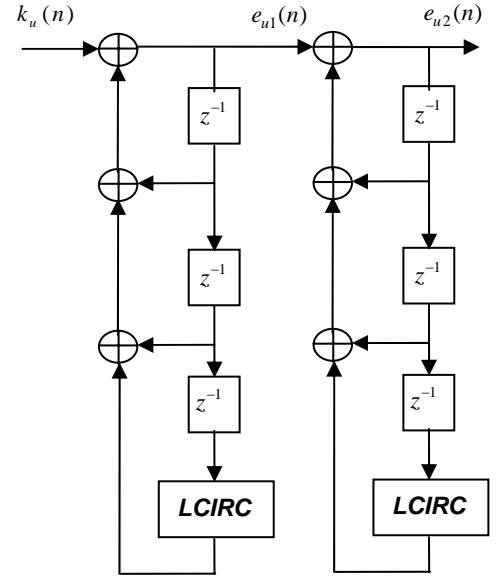


Figure 2: Two cascaded Frey map

2.3. Generator using logarithmic function as a NLF

The equations of the proposed generator are written as follows (see figure 3) [WAN 08]:

$$e_u(n) = \text{mod}\{k_u(n) + \text{mod}\{x_1(n) + \text{mod}[x_2(n), 1], 1\}, 1\}$$

$$e_u(n) = \text{mod}[k_u(n) + x_1(n) + x_2(n), 1]$$

$$x_1(n) = e_u(n-1)$$

$$x_2(n) = \text{Ln}[e_u(n-2)], \quad 0 < e_u(n-2) < 1$$

$$x_1(n) = e_u(n-1)$$

$$x_2(n) = \text{Ln}[e_u(n-2)], \quad 0 < e_u(n-2) < 1$$

(19)

$$e_u(n) = \text{floor}\{\text{mod}\{k_u(n) + e_u(n-1) + \text{Ln}[e_u(n-2)], 1\} * 2^N\} \quad (20)$$

The mod 1 operator imposes $0 < e_u(n-2) < 1$. Combining these equations, we obtain:

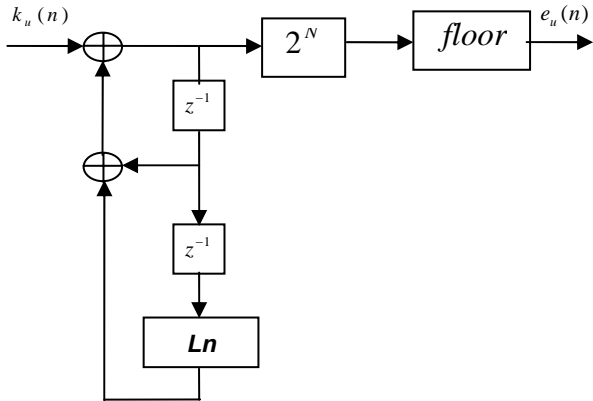


Figure 3: Structure using logarithmic function

3. Comparative simulation results

In order to verify results and compare cryptographic properties of different generators, some experiments were done. The finite computing precision is $N = 32$ bits. The primitive polynomial is given by: $x^{16} + x^{15} + x^{13} + x^4 + 1$ ($k = 16$). The perturbing interval is $\Delta = 99$. Both initial conditions and control parameters are generated randomly. A large number of sampled values are simulated (100000 samples). For example, the following parameters and initial conditions have used:

$$T_{ch} = 5ns ; \quad k_u(n) = 0 ; \quad x_1(0) = 20000 ; \\ x_2(0) = 400 ; x_3(0) = 8000000 \quad \text{and} \quad x_1(0) = 20002 ; \\ x_2(0) = 402 ; x_3(0) = 8000001$$

To verify the balance property, a set of 500 sequences for each chaotic generator are computed, each sequence containing 100000 \times 32 bits.

For all generators under tests, we found that the time domain variation of output signals, the spectrums (DFT), the autocorrelation functions and cross-correlation functions are clearly noise-like.

Figures 4), 5), and 6) represent the DFT spectrum, the autocorrelation function, the cross-correlation function and the attractor for the Frey map with three delays. The percentages of zeros and ones are 55% and 45% respectively.

In figures 7), 8) and 9) we show the DFT spectrum, the autocorrelation function the cross-correlation function and the attractor of perturbed Frey map, which are more random signal compared with results of figures 5), 6). The percentages of zeros and ones are # 50%.

Roughly, we obtain the same results of cascaded two Frey map by including to Frey map with three delays, the perturbation technique described in

paragraph 2, or by using a logarithmic function as a non-linear function (see figure 3).

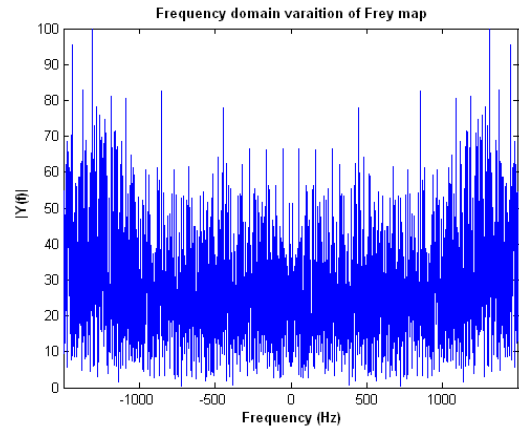


Figure 4: DFT spectrum of Frey map

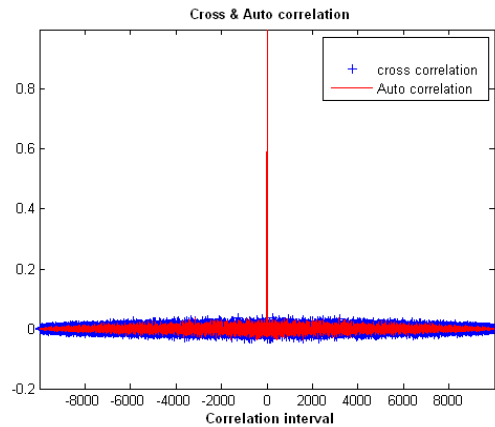


Figure 5: Auto and Cross correlation of Frey map

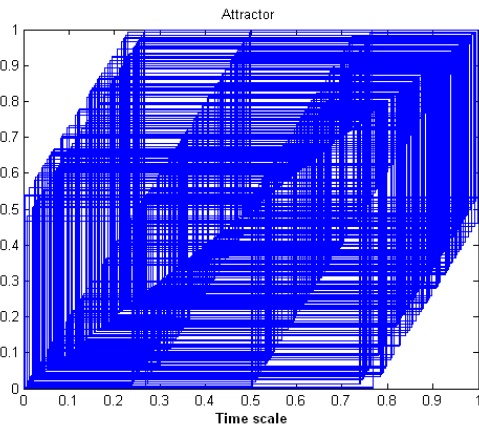


Figure 6: Attractor of Frey map

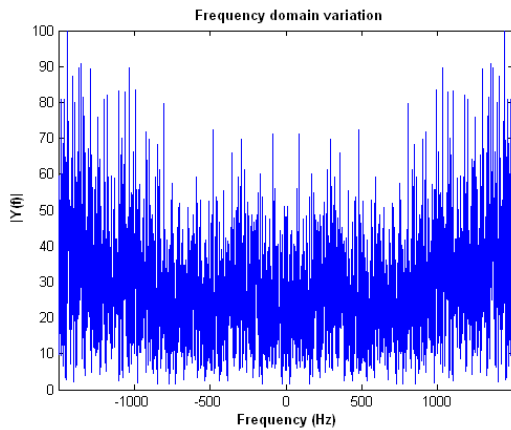


Figure 7: DFT spectrum of perturbed Frey map

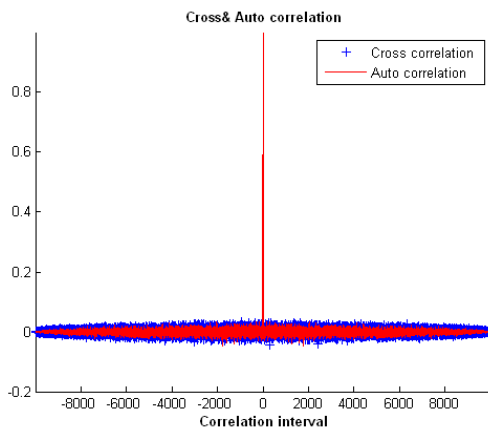


Figure 8: Auto & cross correlation of perturbed Frey map

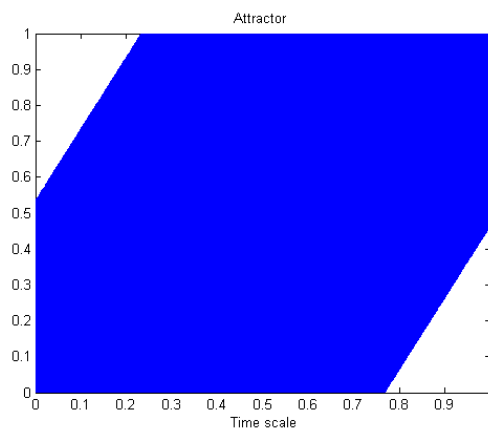


Figure 9: Attractor of perturbed Frey map

Table 1 shows the obtained results of the NIST statistical tests [RUK 01] of studied generators.

Table 1: NIST tests

Statistical tests	Frey map with three delays		Perturbed Frey map		Two cascaded Frey map and Ln function	
	P-val	%	P-val	%	P-val	%
	0.77	73	0.95	92	0.99	98

We use 100 samples of 10^6 bit sequences for each

test. From this table, we can conclude that Frey map with two cascaded stage, generator with logarithmic function and perturbed Frey map are suitable for using in crypto-systems based chaos.

4. Conclusion

In a crypto-system, the use of a good chaotic generator, with desirable dynamical statistical properties, is very important. In this paper, we have developed and implemented under Matlab/Simulink four 1-D dimensional chaotic generators. A comparative analysis of performances using standard criteria between these generators proves the efficiency of the perturbed and cascading techniques. As prospect of this work, we are working on a generator structure whose cycle length is as big as needed.

ACKNOWLEDGMENT

The authors wish to thank the “**Fédération AtlanSTIC – CNRS FR2819**”. This work was supported by the AtlanSTIC research cluster.

REFERENCES

[RUK 01] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, (2001). “A Statistical Test Suite For Random and Pseudorandom Number Generators FOR CRYPTOGRAPHIC APPLICATIONS”. NIST Special Publication 800-22 (with revisions dated May 15, 2001).

[FRE 93] D. R. Frey “Chaotic digital encoding: an approach to secure communications,” *IEEE Transactions on Circuits and Systems II*, vol. 40, pp. 660-666, 1993.

[TAO 98] S. Tao, W. Ruilli, Y. Yixun, “Perturbance based algorithm to expand cycle length of chaotic key stream,” *Electronics Letters*, 34(9):pp. 873-874, 1998.

[ASS 06] S. El Assad, C. Vladeanu, “Digital chaotic codec for DS-CDMA Communication Systems,” *Lebanese Science Journal*, vol. 7, No. 2, 2006.

[ASS 06] S. El Assad, “Communications Numériques: Techniques Avancées,” cours 5ème année, à Polytech’Nantes, 2008.

[WAN 08] Q. Wang “Performances of some Digital Chaotic Generators under NIST tests”, Master2R SEGE, Polytech’Nantes, , 2008.

[TAN 04] W. P. Tang, H. K. Kwan, « Chaotic communications using nonlinear transform-pairs », *ISCAS-2004*, pp, V-740-743, 2004.