Security
of Infocommunication Systems
and Internet of Things

2023 Vol 1, No 2

https://doi.org/10.31861/sisiot2023.2.02010

Received 17 November 2023; revised 26 December 2023; accepted 29 December 2023; published 30 December 2023

Periodicity of Timeseries Generated by Logistic Map. Part I

Oleh Krulikovskyi[1,2,3,*] and Serhii Haliuk[3]

[1]Integrated Center for Research, Development and Innovation in Advanced Materials, Nanotechnologies and Distributed Systems for Fabrication and Control, Stefan cel Mare University of Suceava, 720229 Suceava, Romania
[2]Faculty of Electrical Engineering and Computer Science, Stefan cel Mare University of Suceava, 720229 Suceava, Romania
[3]Department of Radioengineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: o.krulikovskyi@chnu.edu.ua)

ABSTRACT In the paper, the periodicity of pseudo-chaotic implementations in fixed-point calculations is studied using the example of a logistic equation. It was established that with 32-bit represented numbers (three bits - the whole part, 29 bits - the fractional part), the maximum length of the observed cycle is $L_{max} < 2^{14}$ iterations, and the space of possible states of the chaotic system after the completion of the transition process is limited $S \approx 2^{14}$ different numbers. Histograms of the duration of transient processes preceding the exit of the trajectory into a cyclic orbit are constructed. It was found that the maximum durations of the transition process do not exceed $(2L_{max}, 4\,L_{max})$. The paper also demonstrates and substantiates the expediency of using a dynamic threshold when forming binary sequences based on chaotic numbers using the threshold method. It is shown that the criterion for the balance of the binary representation of chaotic sequences enables the optimal choice of the number of high-order bits that must be discarded in order to obtain a uniform distribution. Approaches to increase the cyclicity of period of digital implementations of chaotic systems are analyzed. It is shown that the period of the external disturbance must be coordinated with the durations of the cycles observed in the chaotic system. The results of the work show the limitations of chaotic systems, which must be correctly taken into account when using them in cryptography.

KEYWORDS periodicity, timeseries, logistic map.

I. INTRODUCTION

The applied application of the mathematical apparatus of the theory of nonlinear dynamical systems is an active research field in various disciplines. This is due to the characteristics of the same dynamic systems: ergodicity, sensitivity to initial conditions and parameters, and non-periodicity of the system. This is especially true for various communication systems, as evidenced by the publications in this area. Scientists are trying to use both continuous and discrete nonlinear systems to develop various random and pseudo-random signal generators. The main difficulty in building applications based on such systems is the consistency of parameters in circuit implementation and proving the advantage in performance and resistance to cryptanalysis [1].

Also, one of the important factors for any system in the hardware and software implementation of computer-based processes is that due to the reduction of the set of possible states, chaotic systems lose their "chaotic" character, and their implementations are pseudo-chaotic and cyclic [2-6]. To minimize the impact of this factor, it is necessary to use the maximum possible accuracy of the platform's calculations and take into account the speed of such solutions. Incomplete compliance of basic software and hardware media often leads to the impossibility of reproducing identical pseudo-chaotic implementations on different platforms (different operation systems, programming languages, compilers, different Field-Programmable Gate Array manufacturers).

When performing arithmetic operations on real numbers in floating-point arithmetic [7], there is a factor of different values of rounding error, which, due to the sensitivity of nonlinear systems, leads to divergent trajectories for different hardware and compilers. Hardware-implemented solutions using fixed-point arithmetic make it possible to obtain the same values of chaotic signals (including those with arbitrary time delays) in a spaced manner, which makes it possible to synthesize pseudorandom sequence generators for broadband communications.

II. DISTRIBUTION OF TIMESERIES GENERATED BY LOGISTIC MAP

The peculiarity of chaotic systems is the different frequency of visits of their trajectories to different regions of phase space, which is characterized by fractional values of fractal dimensions. This results leads to an uneven distribution of sequence values generated by such systems.

For the experiment, we will use the logistic map [8] described as discrete-time map:

$$x_{n+1} = rx_n(1 - x_n), \qquad (1)$$

where $x_n \in (0,1)$ and r parameter in the interval (0, 4].

This mapping is well-known and well-studied by other researchers, so we will mention its features here. Using the example of the logistic equation (1), we will point out the problematic issues of using one-dimensional systems as the basis of the pseudorandom number generator.

The histogram of the distribution of timeseries obtained using (1) is shown in Fig. 1. As follows from Fig. 1, the distribution is uneven in the entire range of values of the parameter r, which is undesirable for the implementation of high-quality cryptographic tools. The direct use of solutions (1) as pseudorandom numbers causes their instability to statistical attacks [9].

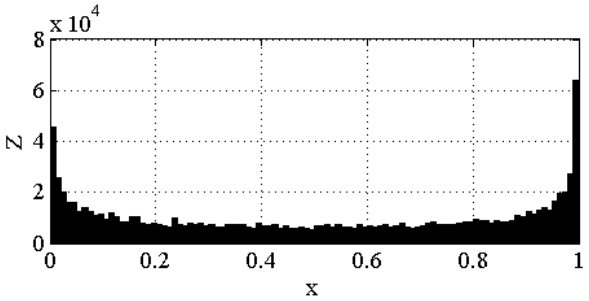


FIG. 1. The histogram of the values of the timeseries generated by (1) at $r = 3.999$ and $n = 1000000$.

The simplest way to obtain a pseudo-random sequence using (1) is the threshold method [10], according to which the phase space of the system is divided into two independent regions corresponding to the binary symbols "0" or "1":

$$X(n) = \begin{cases} 0, & x_n \le x_t \\ 1, & x_n > x_t' \end{cases} \qquad (2)$$

where x_t – threshold value.

The dependence of the percentage of "1" symbols in the sequence obtained according to (1) and (2) on the value of the control parameter r is shown in Fig. 2.

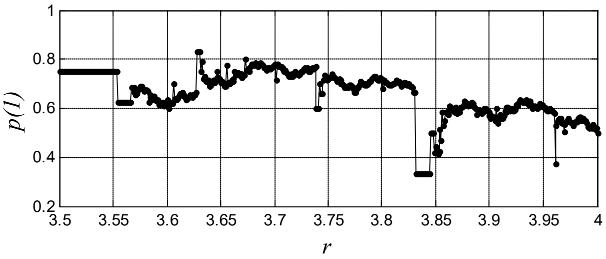


FIG. 2. Dependence of the probability of obtaining the symbol "1" by the threshold method at $x_t = 0.5$ on the control parameter r.

As we can see, the shares of symbols "0" and "1" when choosing a threshold differ significantly, which indicates an imbalance of the sequence.

The disadvantage of the threshold method can be eliminated by dynamically selecting the threshold, as the median of the distribution at a given value of the control parameter (Fig. 3).

Another disadvantage of the threshold method is also the low speed of generating a pseudo-random sequence, since it is possible to obtain only one bit of the sequence in one iteration. It is possible to increase the speed of generating a pseudo-random sequence by utilizing bitwise representation of random numbers.

The histogram of any chaotic system when implemented by software on a computer is formed by the significant bits of the binary representation of data. By discarding a part of the bits that do not meet the balance criterion, sequences with a uniform distribution can be obtained.

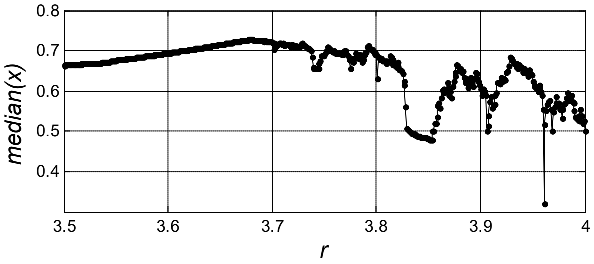


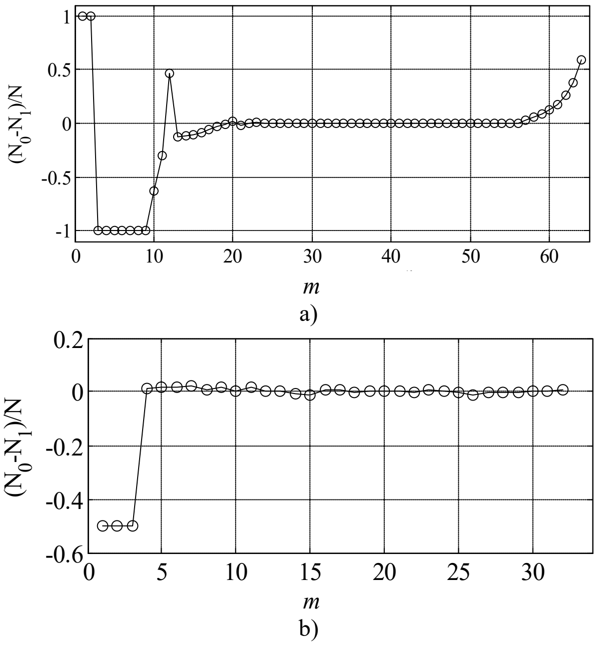
FIG. 3. Dependence of the median of the distribution of system implementations (1) on the control parameter r.

Let's consider the features of the bitwise representation of numbers in calculations with double precision and fixed and floating point calculation. Chaotic sequence can be represented as a matrix with dimension $n \times m$ and elements $l_{n,\ m}$.

$$\left\{\begin{matrix} l_{11}\ . & l_{12} & \dots & l_{1,\ m} \\ l_{21}\ . & l_{22} & \dots & l_{2,\ m} \\ . & . & \dots & . \\ l_{n,1}\ . & l_{n,2} & \dots & l_{n,\ m} \end{matrix}\right. , \qquad (3)$$

where n – number of iteration x_n, and m - the sequence number of a bit in the binary representation of a real number.

For each column, the number of zeros "0" - N_0 and ones "1" - N_1 is calculated. Accordingly, $(N_0 + N_1 = N)$.. The dependence of the relative difference of the number of "0" and "1" to the whole number of the binary symbol is shown in Fig. 4. The notation Q3.29 means that we used 32 bit fixed point arithmetic with 29 bits for fractional part and 3 bits for integer part.



a)

b)

FIG. 4. Balanced sequences for the logistic equation: (a) at r = 3.999 for double precision; (b) arithmetic Q3.29.

As can be seen from Fig. 4,*a*, for double precision, the most significant bits that form the chaotic attractor (1) are unbalanced. The deviation in the proportion of "0" and "1" for the least significant bits is due to the peculiarities of rounding in floating-point arithmetic. The lower bits are balanced when implementing logistic mapping on a FPGA

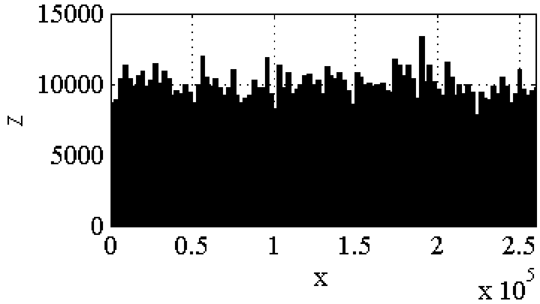


FIG. 5. Histogram of values of timeseries generated by (1) at r = 3.999, n = 1000000 when discarding the oldest 15 bits at Q3.29.

and in computer calculations using fixed-point arithmetic (Fig. 4,*b*). Histogram of pseudorandom numbers obtained on the basis of implementations (1) by discarding the highest 15 bits is given in Fig. 5. We can see a uniform distribution, which proves consistency of our approach.

True chaotic signals can be obtained only in an analog dynamic system [2]. In computer simulation, regardless of the calculation format, the obtained realizations of chaotic signals will be pseudo-chaotic, that is, they will be repeated (the repetition period can be large), since computers are characterized by a finite number of states.

With a quite large repetition period, the solutions of the chaotic system will preserve the dimensionality, ergodicity and properties of the real attractor. This makes it possible to study chaotic systems by modeling them [11]. The number of cycles at one value of the parameter is limited, due to the fact that a large number of trajectories formed under different initial conditions, after the end of the transition process, reach the same discrete periodic orbits [4]. Due to the cyclic nature of the pseudo-chaotic sequence, the amount of information to be encrypted and the key space of the method are limited.

There are several ways to extend period of pseudo-chaos that include increasing the precision of calculations, periodic disturbances and using multidimensional systems.

An increasing of calculations accuracy is possible when using expensive hardware, which is a significant restraining factor, and software implementation requires an increase in time costs.

The effectiveness of periodic disturbances depends on the properties of the system to which they are applied, the nature of the disturbances and their frequency. For example, consider the logistic map (1), if the duration of the cycle of a chaotic system is one iteration [2], disturbances with a repetition period longer than the average duration of the transition process are inappropriate, since they will lead to the periodic repetition of part of the same trajectory. The temporal implementation of system (1) in arithmetic Q3.9 under the influence of a random periodic disturbance every 50 iterations is shown in Fig. 6.

From Fig. 6 it follows that the impact of the perturbation causes a short transient process, after which the system collapses or enters a periodic orbit. A similar situation will occur if the average duration of the cycles is shorter than the period of influence of the disturbance.

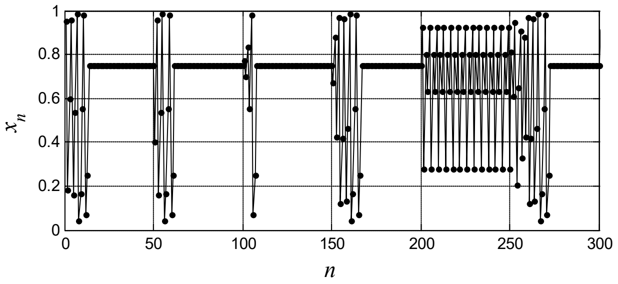


FIG. 6. Repeatability of collapse under random periodic perturbations after every 50 iterations.

III. PERIODICITY OF LOGISTIC MAP TIMESERIES WITH LIMITED PRECISION OF ARITHMETIC CALCULATIONS Q3.29

The influence of the accuracy of the representation of numbers on the crypto resistance of data encryption methods was partially investigated in [9]. In [12], numerical simulation was used to show that the rounding of numbers during the iteration of a chaotic system leads to the occurrence of periodic oscillations. At the same time, the repetition period is much smaller than the cardinality of possible states of the system. The periodicity of realizations of digitized chaotic systems is the reason for reducing the power of the set of values of initial conditions and control parameters in chaos-based encryption system.

When performing calculations in the fixed-point format, the set of solutions is the amount of numbers that differ by at least one binary digit, which is equal to 2^{m+d}, where m and d - are the digital representation of the fractional and integer part of the number, respectively (including the sign) . If calculations are carried out with a floating point, then the periodicity of solutions will depend on the features of the hardware and (or) software.

Despite the fact that the problem of the impact of calculation precision on the properties of implementations of chaotic systems is known, it is often not taken into account when evaluating the cryptoresistance of the proposed methods.

Length of cycles of logistic map (1) for different values of the control parameter when using fixed-point arithmetic Q3.29 are given in the Table. 1.

In the simulation, 10^5 random initial conditions with a uniform distribution of their values were set. The repetition period of the sequences generated by (1) is significantly less than the maximum possible. After the end of the transition process at m = 32, the number of different sequences that can be generated using (1) is limited and does not depend on the initial conditions. This means that the use of initial conditions as a key in individual cryptographic algorithms is not always appropriate.

For different values from the Table. 1. it follows that changing the control parameter does not significantly change the cycle period, but the generated sequence does. If we analyze the chaotic sequence formed by logistic map (1), we see that after the end of the transient process, the value of the parameter r, is more informative, than an initial condition $x(0)$.

TABLE 1. Lengths of periods of logistic map.

The value of the parameter, *r* (in hexadecimal)	*L*	Number of initial conditions
80000000	6876	94672
	571	1086
	379	4206
	327	36
7fffffff	14561	58534
	4133	16435
	3331	18174
	1499	6442
	932	373
	193	34
	82	7
	13	1
7ffffffe	9215	97141
	4627	2091
	2564	680
	488	25
	300	42
	289	13
	136	3
	129	3
	17	2
7ffffffd	11078	51659
	3167	32673
	1230	651
	1177	14681
	362	317
	77	5
	29	2
	21	11
	13	1

For systems with infinite computational precision, sensitivity to initial conditions and parameter values are equivalent in the sense that perturbations of both lead to different realizations of the chaotic process. With restrictions on the accuracy of calculations from the point of view of chaotic cryptography, it can be concluded that the sensitivity to the parameter values is higher than to the initial conditions. This must be taken into account when developing chaotic encryption algorithms. Moreover, software-implemented chaotic systems are insensitive to initial conditions that differ by the minimum possible value of 2^{-m} if, after one or more iterations, their trajectories completely coincide [13].

The maximum length of the transient process of system (1) with r=4-2^{-29} and Q3.29 was 16775 iterations (Fig. 7).

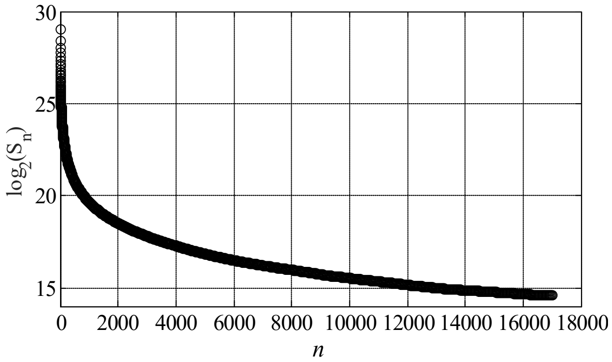
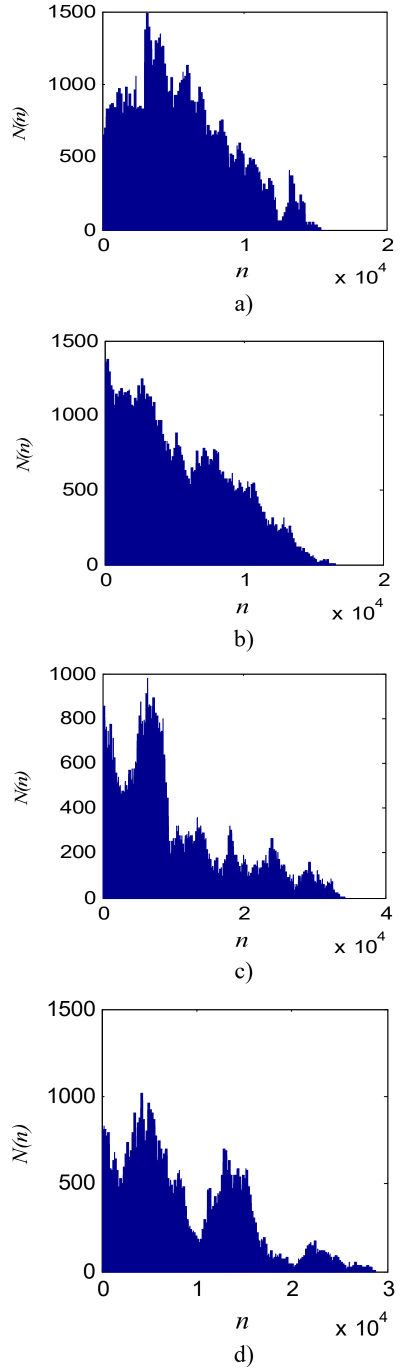


FIG. 7. Dependence of the cardinality of the set of possible states of the logistic equation on the number of iterations, *n*.

As a result of strong degradation, the power of the set of different initial conditions in 2^{29} after the transition process is equal to the sum of the lengths of all possible cycles 24797≈2^{14}. The distribution of the duration of the transient process depends on the value of the control parameter r and is uneven (Fig. 8). It follows from the simulation results that the maximum duration of the transition process is limited to $(2L_{max}, 4\,L_{max})$.

According to the Kerckhoffs principle, the attacker knows everything about the encryption method except the keys. Therefore, rejecting the transitional process to increase the security of a chaotic cipher, as, for example, is proposed in pioneering works on chaos-based



a)

b)

c)

d)

FIG. 8. Histogram of the distribution of the duration of transient processes: (a) at $r = 4$, (b) at $r = 4 - 2^{-29}$, (c) at $r = 4 - 2 \times 2^{-29}$, (d) at $r = 4 - 3\ \times 2^{-29}$.

cryptography [7,9] is meaningless. If an attacker breaks the cipher with a brute-force attack, the key for him will be the values of the parameters and the initial conditions of the chaotic system at the time of encryption.

As shown in works [14-15] (mostly at a qualitative level), due to dynamic degradation, the repetition period of pseudo-chaos is very small compared to the maximum possible.

IV. CONCLUSION

In the work, the periodicity of pseudo-chaotic implementations in fixed-point calculations is studied using the example of a logistic equation. It was established that with 32-bit represented numbers (three bits - the whole part, 29 bits - the fractional part), the maximum length of the observed cycle is $L_{max} < 2^{14}$ iterations, and the space of possible states of the chaotic system after the completion of the transition process is limited $S \approx 2^{14}$ different numbers. Histograms of the duration of transient processes preceding the exit of the trajectory into a cyclic orbit are constructed. It was found that the maximum durations of the transition process do not exceed $(2L_{max}, 4\,L_{max})$. The paper also demonstrates and substantiates the expediency of using a dynamic threshold when forming binary sequences based on chaotic numbers using the threshold method. It is shown that the criterion for the balance of the binary representation of chaotic sequences enables the optimal choice of the number of high-order bits that must be discarded in order to obtain a uniform distribution. Approaches to increase the cyclicity of period of digital implementations of chaotic systems are analyzed. It is shown that the period of the external disturbance must be coordinated with the durations of the cycles observed in the chaotic system.

AUTHOR CONTRIBUTIONS

O.K. – investigation and validation, resources, Simulink implementation and testing, writing-original draft preparation, supervision; S.H. – results discussion, draft preparation and additional support.

COMPETING INTERESTS

The authors declare that they have no conflict of interest.

REFERENCES

[1] Sato A., Endo T. Experiments of Secure Communications Via Chaotic Syncronization of Phase-Locked Loops // IEEE Trans Fundamental. Vol E78-A, No 10, Oct, 1995.p.l286-1290.

[2] Yuan G. Collapsing of chaos in one dimensional maps / G. Yuan, J.A. Yorke // Physica D: Nonlinear Phenomena. – 2000. - №136. – pp. 18-30.

[3] Fei Yu, Lixiang Li, Qiang Tang, Shuo Cai, Yun Song, and Quan Xu, “A Survey on True Random Number Generators Based on Chaos”, Discrete Dynamics in Nature and Society, Vol. 2019, A. ID 2545123, 2019.

[4] Hans Thunberg, “Periodicity versus Chaos in One-Dimensional Dynamics”, SIAM Review, vol. 43(1), pp. 3-30, 2001.

[5] M. Joglekar, E. Ott, James A. Yorke, “Scaling of Chaos versus Periodicity: How Certain is it that an Attractor is Chaotic?”, Phys. Rev. Lett., vol. 113(8), p. 084101(4), 2014.

[6] M. Sobottka, Luiz P. L. de Oliveira. “Periodicity and Predictability in Chaotic Systems.” The American Mathematical Monthly 113(5), pp. 415–24, 2006.

[7] Ljupco Kocarev Chaos-Based Cryptography Theory, Algorithms and Applications / L. Kocarev, S. Lian. Berlin: Springer-Verlag Berlin Heidelberg, 2011. - 397 pp.

[8] May, R. Simple mathematical models with very complicated dynamics. Nature 261, 459–467 (1976).

[9] Alvarez G. Some basic cryptographic requirements for chaos-based cryptosystems / G. Alvarez, Li S.J. // International Journal of Bifurcation and Chaos. – 2006. - 16 (8). - pp. 2129-2151.

[10] Zhang Xuefeng Extended Logistic Chaotic Sequence and Its Performance Analysis / Zhang Xuefeng, Fan Jiulun // Tsinghua science and technology. – 2007. - Volume 12, Number S1. - pp156-161.

[11] Haliuk, S.; Krulikovskyi, O.; Vovchuk, D.; Corinto, F. Memristive Structure-Based Chaotic System for PRNG. Symmetry 2022, 14, 68.

[12] Harris Bernard Probability Distributions Related to Random Mappings / Bernard Harris // Ann. Math. Statist. – 1960. - Volume 31, Number 4. pp. 1045-1062.

[13] Haliuk, Serhii, et al. "Circuit implementation of Lozi ring-coupled map." 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). IEEE, 2017.

[14] Harris Bernard Probability Distributions Related to Random Mappings / Bernard Harris // Ann. Math. Statist. – 1960. - Volume 31, Number 4. pp. 1045-1062.

[15] Celso Grebogi Roundoff-induced periodicity and the correlation dimension of chaotic attractors / Celso Grebogi, Edward Ott, and James A. Yorke // Phys. Rev. – 1988. - A 38, 3688.

Oleh Krulikovskyi

Assistant professor at Radio Engineering and Information Security Department of Chernivtsi National University. His research field covers digital signal processing, FPGA and hardware cryptography. Author of more than 20 publications.

ORCID ID: 0000-0003-3836-2675

Serhii Haliuk

Assistant professor at Radio Engineering and Information Security Department of Chernivtsi National University. His research interest covers the development of the different components of hidden communication systems. Author of more than 30 publications.

ORCID ID: 0000-0001-5995-6857

Періодичність цифрової реалізації логістичного рівняння. Частина I

Олег Круліковський [1,2,3,*], Сергій Галюк[3]

[1]Інтегрований центр досліджень, розробок та інновацій у галузі передових матеріалів, нанотехнологій і розподілених систем для виготовлення та керування, Сучавський університет імені Штефана чел Маре, 720229 Сучава, Румунія
[2]Факультет електротехніки та комп'ютерних наук, Сучавський університет імені Стефана чел Маре, 720229 Сучава, Румунія
[3]Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: o.krulikovskyi@chnu.edu.ua)

АНОТАЦІЯ При переході до апаратно-програмної реалізації процесів на базі ЕОМ внаслідок зменшення множини можливих станів хаотичні системи втрачають «хаотичність», а їх реалізації є псевдохаотичними і циклічними. Відповідно це є особливо важливим при розробці нових додатків на базі нелінійних систем в галузі комунікацій та інформаційних технологій. Проблема періодичності хаотичних систем при програмній реалізації безпосередньо впливає на криптографічну стійкість та складність атаки грубої сили на хаотичні алгоритми шифрування. У роботі на прикладі логістичного рівняння вивчається періодичність псевдохаотичних реалізацій при обчисленнях з фіксованою комою. Встановлено, що при 32-бітному представлені чисел (три біти - ціла частина, 29 біт - дробова частина) максимальна довжина циклу, що спостерігався становить $L_{max} < 2^{14}$ ітерацій, а простір можливих станів хаотичної системи після завершення перехідного процесу обмежується $S \approx 2^{14}$ різних чисел. Побудовано гістограми тривалості перехідних процесів, що передують виходу траєкторії на циклічну орбіту. Виявлено, що максимальні тривалості перехідного процесу не перевищують $(2L_{max}, 4\,L_{max})$. Також у роботі продемонстровано та обґрунтовано доцільність використання динамічного порогу при формуванні двійкових послідовностей на основі хаотичних чисел пороговим методом. Показано, що критерій збалансованості двійкового подання хаотичних послідовностей, уможливлює оптимальний вибір кількості старших біт які необхідно відкинути щоб отримати рівномірний розподіл. Проаналізовано підходи щодо збільшення періоду повторення цифрових реалізацій хаотичних систем. Показано, що період зовнішнього збурення необхідно узгоджувати з тривалостями циклів, що спостерігаються у хаотичній системі. Результати роботи показують обмеження хаотичних систем, що необхідно коректно враховувати при їх застосуванні в криптографії.

КЛЮЧОВІ СЛОВА періодичність, часові ряди, логістичне відображення.

This article is licensed under a Creative Commons Attribution 4.0 International License. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.