Security of Infocommunication Systems and Internet of Things

2024 Vol 2, No 2

https://doi.org/10.31861/sisiot2024.2.02003

Received 06 September 2024; revised 20 October 2024; accepted 19 November 2024; published 30 December 2024

Periodicity of Timeseries Generated by Logistic Map: Part II

Oleh Krulikovskyi[1,2,3], Serhii Haliuk[1,*], Viktor Ivashko[4] and Ruslan Politanskyi[1]

[1]Department of Radioengineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine
[2]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
[3]Faculty of Electrical Engineering and Computer Science, Stefan cel Mare University of Suceava, 720229 Suceava, Romania
[4]Department of Computer Science, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: s.haliuk@chnu.edu.ua)

ABSTRACT The paper investigates the impact of limited computational precision on chaotic systems used in cryptography, focusing on how floating-point arithmetic influences the periodicity and degradation of chaotic timeseries. The study analyses the behaviour of logistic map, revealing that different initial conditions and parameters lead to varying cycle lengths, which are critical for maintaining chaos in encryption algorithms. The order of arithmetic operations and the choice of coupling methods between maps are shown to significantly affect the system's dynamics. The efficiency of using floating-point and fixed-point arithmetic is compared, demonstrating that precision limitations can lead to the degradation of chaos, thereby compromising the effectiveness of some chaos-based ciphers. The research provides insights into the behaviour of chaotic systems under computational constraints, aiming to improve the reliability and security of chaotic encryption techniques.

KEYWORDS periodicity of chaos, chaotic timeseries, logistic map.

I. INTRODUCTION

Chaotic cryptography remains the key topic of applied chaos [1-4]. The necessity to protect huge amount of information requires fast and reliable real-time encryption, putting restrictions on computational cost and power consumption. Recently proposed chaotic encryption algorithms aim to increase data security and not to be complex computationally. Numerous studies have proposed to leverage such systems for the development of various information security techniques. However, relatively little attention has been focused on the practical implementation of nonlinear dynamical systems and the influence of digital computing on system dynamics [5-7].

The impact of limited computational precision on time series generated by discrete maps has substantial practical relevance for a wide array of applications based on nonlinear discrete-time dynamical systems [8-12].

Chaos-based cryptography mostly uses timeseries, which are real numbers obtained by digital mathematical operations made over chaotic systems. Fixed-length size of word of digital tools simplifies chaotic dynamics, leading to its degradation and periodicity. Our previous work showed that logistic map with fixed-point 32-bit precision of calculation has cycles no more than 2^{14} long [8].

This work is a continuation of the research [8] and presents the results of studying the impact of computational precision limitations on the dynamics of a chaotic system when using floating-point arithmetic. The aim is to reveal a better understanding of the degradation of nonlinear dynamical systems for their software implementation in chaos-based ciphers.

The dynamic degradation of digital timeseries is usually studied by rounding numbers in decimal format after each iteration of chaotic system [9-10]. In this paper, we concentrate on studying the behaviour of chaotic map using IEEE 754 floating-point double-precision arithmetic as it is. This allows us to estimate the true influence of dynamic degradation on length of cycles, which can affect chaotic encryption techniques.

The paper is organized as follows. In section II we study the impact of floating-point arithmetic on the periodicity of logistic equation iterations. The role of the order of arithmetic operations is studied in Section III. The behaviour of weakly coupled logistic maps is revealed in Section IV. The efficiency of using different types of arithmetic is discussed in Section V. In Section VI, the internal causes of the degradation of the logistic equation dynamics are explained. Conclusions are provided in Section VII.

II. PERIODICITY OF LOGISTIC MAP TIMESERIES WITH DOUBLE PRECISION ARITHMETIC

Double precision is a floating-point number format established by IEEE as IEEE 754 standard [13, 14]. Differently from fixed-point format, which ensures constant absolute error, floating-point format benefits with constant relative error, providing better precision of computation when working with small numbers. According to IEEE 754, double-precision numbers occupy 64 bits in a computing device's memory and allow storing numbers between 10^{-308} and 10^{308} with approximately 16 significant digits. The double binary string has one sign bit s, 11 bits as exponent e, 52 bits as fraction part f (Fig. 1). A number in double precision can be described by

$$-1^{s} * 2^{e-1023} * 1.f. \quad (1)$$

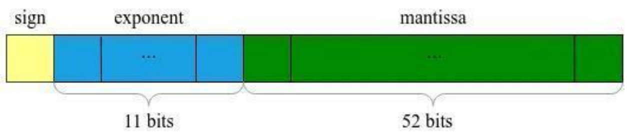


FIG. 1. The structure of double number in memory.

Double precision applications encompass scientific computing, engineering simulation, financial modelling and other fields. In the context of chaos encryption, double-precision arithmetic is the primary format for representing the raw output of chaotic systems.

We continue to study logistic map which is described by

$$x_{n+1} = rx_n(1 - x_n), \quad (2)$$

where $x_n \in (0,1)$ and r is the parameter within the interval (0, 4). The value range of r when chaos can occur is shorter $r \in (3.75\ 4)$ and includes a lot of periodic windows.

Table 1 shows cycles length of timeseries generated by map (2) with double precision and rounding toward zero. Over 10000 random evenly distributed initial conditions within range (0, 1) were tested. There are small amounts of cycles that appear after transient time in spite of different initial conditions. Transient time in the context of digital chaos refers to the number of iterations required before the trajectory of a chaotic system settles into a repeating loop or cycle. Specifically, it denotes the number of iterations it takes for any number within the series to become part of a cyclical state, starting from a given initial condition. Taking into account that the only minor part of possible initial conditions were used, it cannot be asserted that all possible cycles are found. However, the share of initial conditions, evolving from which the chaotic map falls into other cycles, not indicated in Table 1, is very small.

When $r = 3.99$, the whole 10000 initial conditions result in the same cycle after transient. When $r = 4$, timeseries started from approximately 16.39% of initial conditions collapse to cycles length 1. Relying on data in Table 1, we can conclude that independently of value of r, a few cycles prevail with significant percentage. When $r = 3.98$, the most probable cycle has 22366995 iterations and appears in 99.33% cases.

III. INFLUENCE ORDER OF OPERATION ON DYNAMIC DEGRADATION

In general, floating-point computer arithmetic due to finite precision representation of numbers does not hold associative and commutative properties, which means that for $a, b, c \in R$ the following inequalities hold

$$(a + b) + c \neq a + (b + c), \quad (3)$$

$$a(bc) \neq (ab)c. \quad (4)$$

The computation result can be less than machine epsilon or takes more memory cells to be saved exactly. In both cases, rounding errors appear due to fitting numbers into machine format. Rounding errors issues in degradation of chaos, destroying true chaos dynamic.

While computing with a complex formula, the order of operation affects the final result. It is easy to obtain the following form of logistic map that are equal to (2):

$$x_{n+1} = x_n(1 - x_n)r \quad (5)$$

$$x_{n+1} = (1 - x_n)rx(n) \quad (6)$$

$$x_{n+1} = rx_n - rx_n{}^2 \quad (7)$$

$$x_{n+1} = x_n(r - rx_n) \quad (8)$$

$$x_{n+1} = 1 + x_n(1 - x_n)r - 1 \quad (9)$$

Taking into account the standard order of math operations – parentheses, exponents, multiplication and division, and addition and subtraction – where operations of equal precedence are performed from left to right, it is evident that a digital computer will treat the map (2) and (5-9) differently, producing different timeseries.

TABLE 1. Lengths of cycles of logistic map with double floating-point arithmetic.

The value of the parameter, r	The length of cycle, L	% of initial conditions
$r = 3{,}97$	85622	0.43
	552417	0.01
$(400fc28f5c28f5c3)_{16}$	5044757	53.56
	5313964	41.12
	10494186	4.88
$r = 3.98$	63581	0.03
	993537	0.09
$(400fd70a3d70a3d7)_{16}$	1098807	0.02
	2432720	0.43
	2781805	0.10
	22366995	99.33
$r = 3.99$	6623920	100
$(400feb851eb851ec)_{16}$		
$r = 4$	1	16.39
	420909	0.01
$(4010000000000000)_{16}$	960057	0.01
	1311627	0.02
	2441806	1.51
	2625633	1.63
	5638349	68.15
	10210156	1.69
	14632801	10.59

IV. PERIODICITY OF WEAKLY COUPLED MAPS

Increasing the dimensionality of a chaotic map is a method to generate more complex and less predictable time series. This approach helps counteract the dynamic degradation of chaos in computer systems.

Beginning with one-dimensional chaotic maps, multidimensional maps can be created through dissipative coupling. There are unidirectional and bidirectional techniques for connecting two systems.

The first method describes an interaction between two systems where the influence flows on only one direction and one system is completely independent of the other:

$$x_{n+1} = (1 - \varepsilon)(r_1 x_n(1 - x_n)) + \varepsilon y_n, \quad (10)$$

$$y_{n+1} = r_2 y_n(1 - y_n), \quad (11)$$

where ε is coupling factor or coupling strengths.

The value of ε determines the first system's suppression level by the second. To increase the system's cycle length, the coupling factor ought to be small enough to preserve its inner chaotic dynamic. Large ε can lead to synchronization phenomena, which levels the influence of dimension increase on cycle lengths.

TABLE 2. Lengths of cycles of logistic map with double floating-point arithmetic and different order of operations.

Chaotic system model, $r = 3,99$ $(400feb851eb851ec)_{16}$	**The length of cycle, *L***	**% of initial conditions**
$x_{n+1} = x_n(1 - x_n)r$	133045	0.48
	265827	0.01
	643624	1.38
	1356328	0.03
	12074794	19.01
	68218191	79.09
$x_{n+1} = (1 - x_n)rx(n)$	580343	0.19
	1425160	4.63
	1883848	0.2
	12268155	0.98
	28363422	94.0
$x_{n+1} = rx_n - rx_n{}^2$	341935	0.01
	1372203	0.16
	5811754	46.66
	6543850	34.42
	10128220	7.76
	14303402	11.99
$x_{n+1} = x_n(r - rx_n)$	2153214	0.06
	3951504	0.6
	30953002	99.34
$x_{n+1} = 1 +$	173381	0.09
	216679	0.09
$+ x_n(1 - x_n)r - 1$	9368067	35.4
	11705492	64.42

Fig. 2 illustrates the synchronization phenomenon. When $\varepsilon = 0.3$, the connected systems (11) and (12) produce time series with significant differences between the values of their iterations (see Fig. 2a,b). Unidirectional synchronization occurs at $\varepsilon = 0.6$, resulting in errors that are nearly machine-zero, with the cycle length of system (10) being determined by system (11) (see Fig. 2c,d).

The second coupling method refers to an interaction between two systems when they disturb each other's dynamics. The model of the bidirectional coupling of logistic maps is following

$$x_{n+1} = (1 - \varepsilon_1)(r_1 x_n(1 - x_n)) + \varepsilon_1 y_n, \qquad (12)$$

$$y_{n+1} = (1 - \varepsilon_2)(r_2 y_n(1 - y_n)) + \varepsilon_2 x_n. \qquad (13)$$

The coupling factors ε_1 and ε_2 should be chosen to prevent complete chaos synchronization, when x_n and y_n become equal, or parameter r_1 and r_2 should be different.

Using the simulation of systems (12) and (13) with $\varepsilon = 0.3$, we unsuccessfully attempted to identify the repetition period of the sequences. Upon examining sequences up to a length of 10^{16} cycles, no periodicity was detected, indicating that the average total duration of the transient process and the cycle exceeds 10^{16} iterations.

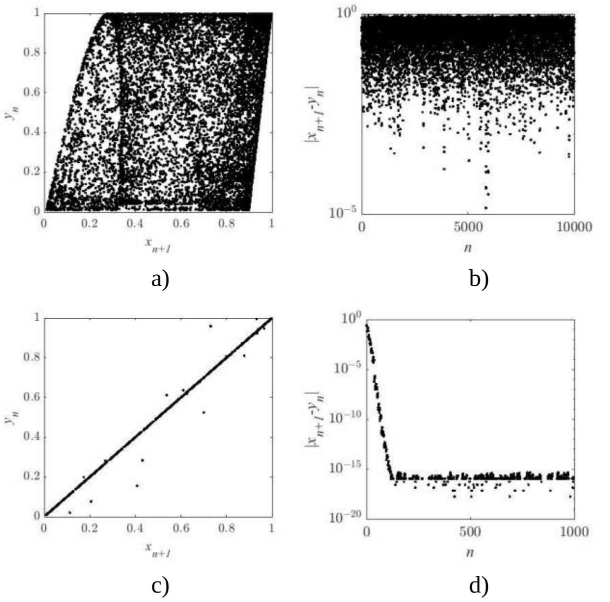


FIG. 2. The synchronization phenomena: (a) desynchronization and (b) error $|x_{n+1} - y_n|$ when $\varepsilon = 0.3$, (c) synchronization and (d) error $|x_{n+1} - y_n|$ when $\varepsilon = 0.6$.

V. EFFICIENCY OF DIFFERENT ARITHMETICS

The efficiency of using floating-point arithmetic depends on the size of the phase space where chaotic attractor exists and the maximum and minimum numbers that the computing machine operates with during calculations. The advantages of floating-point arithmetic can be reduced if the solutions of chaotic systems do not cover the entire set of permissible numbers.

For system (2), the permissible values of initial conditions are restricted inside the range (0, 1), regardless of the value of the parameter. However, the range of chaotic realizations after the transient process ends will not exceed a certain interval. With a change in the parameter, both the range of realizations and the key space of initial conditions will change. It is easy to show that maximum and minimum value of x are

$$x_{max} = f(r, 0.5) = \frac{r}{4},$$

$$x_{min} = f(r, x_{max}) = \frac{r^2}{4}\left(1 - \frac{r}{4}\right).$$

The sequence of solutions of system (2), starting from an arbitrary initial condition from the region (0,1), will eventually be bounded by the range $[x_{min}, x_{max}]$, which defines the region of existence of the chaotic attractor of logistic map.

Let us consider the influence of the linear dimensions of the logistic map attractor (post-transient) on the efficiency of using fixed-point and floating-point arithmetic. We use the ratio of the cardinality of the set of permissible numbers of the arithmetic N_0 to the cardinality of the set belonging to the system attractor N as the efficiency measure of arithmetic usage:

$$eff = \frac{N}{N_0}. \qquad (14)$$

For double arithmetic and $r = 4$, the minimum value of x_{min} was chosen equal $x_{min} = 2^{-53}$ such that system (2)

TABLE 3. The efficiency of using different arithmetics for logistic map.

Arithmetic	r	x_{max}	x_{min}	The amount of different numbers N in the range $[x_{min}, x_{max}]$	The amount of different numbers N_0	Efficiency, eff
single	3,75	0.9375 $(3f700000)_{16}$	0.2197265625 $(3e610000)_{16}$	$\approx 2^{24.08}$	$\approx 2^{32}$	$\approx 2^{-7.92}$
	4	1 $(3f800000)_{16}$	2^{-25} $(33000000)_{16}$	$\approx 2^{-27.64}$	$\approx 2^{32}$	$\approx 2^{-4.36}$
double	3,75	0.9375 $(3fee000000000000)_{16}$	0.2197265625 $(3fcc200000000000)_{16}$	$\approx 2^{53.06}$	$\approx 2^{64}$	$\approx 2^{-10.94}$
	4	1 $(3ff0000000000000)_{16}$	2^{-54} $(3c90000000000000)_{16}$	$\approx 2^{57.755}$	$\approx 2^{64}$	$\approx 2^{-6.245}$
fixed-point, 32 bits	3,75	0.9375 $(1e0000000000)_{16}$	0.2197265625 $(07080000)_{16}$	$\approx 2^{28.52}$	2^{32}	$\approx 2^{-3.48}$
	4	1 (20000000)16	0 $(00000000)_{16}$	$\approx 2^{29}$	2^{32}	$\approx 2^{-3}$
fixed-point, 64 bits	3,75	0.9375 $(1e00000000000000)_{16}$	0.2197265625 $(0708000000000000)_{16}$	$\approx 2^{60.52}$	2^{64}	$\approx 2^{-3.48}$
	4	1 $(2000000000000000)_{16}$	0 $(0000000000000000)_{16}$	2^{61}	2^{64}	$\approx 2^{-3}$

preserved its structure. If the value of $x_n < 2^{-53}$, then x_n is considered as machine zero relative to 1, thus $1 - x_n = 1$. In this case, equation (2) is equivalent to the following linear expression:

$$x_{n+1} = r x_n. \quad (15)$$

The impact of the linear size of the logistic map attractor (post-transient) on the efficiency of using fixed-point and floating-point arithmetic is presented in Table 3.

VI. REASONS OF CHAOS DEGRADATION

During the iteration process, the cardinality of the set of possible states in the chaotic system decreases. This phenomenon is driven by two factors:

1. Due to the mixing property, different regions of the initial conditions converge to a single region after iterations. For example, in the case of the logistic map (Fig. 3a), two subintervals are mapped into one:

$$S_{0,1} \to S_{1,1}, S_{0,2} \to S_{1,1},$$
$$S_1 = (S_{1,1} \cup S_{1,2}).$$

If $r = 4$, we obtain:

$$S_1 = f(0, 0.5] \cup f(0.5, 1) = (0,1).$$

As a result of the transformation, the cardinality of the system's different state set decreases by the number of identical elements in $S_{1,1}$ and $S_{1,2}$.

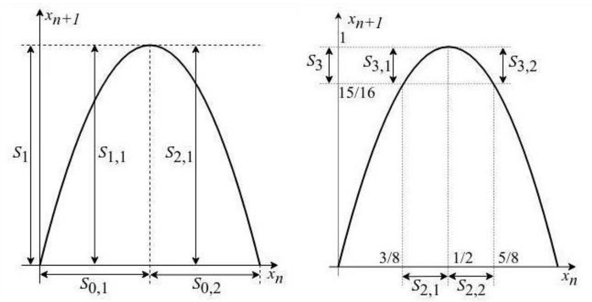
2. Due to the shrinking of the phase space in regions with a negative local Lyapunov exponent. For one-dimensional maps, this region is bounded by points where the absolute value of the derivative is

$$\left|\frac{df(x)}{dx}\right| < 1.$$

The shrinking transformation is shown in Fig. 3b:

$$S_{2,1} \to S_{3,1}, S_{2,2} \to S_{3,1},$$
$$S_3 = (S_{3,1} \cup S_{3,2}).$$

For the logistic map with $r = 4$, the shrinking region is bounded as $\left(\frac{3}{8}, \frac{5}{8}\right)$.



a) b)

FIG. 3. The transformation of phase space of logistic map.

After the first iteration, the set $S_{2,1}$ evolves into $S_{3,1}$, as shown in Fig. 3b, i.e.

$$S_{2,1} = \left(\frac{3}{8}, \frac{1}{2}\right], S_{2,2} = \left(\frac{1}{2}, \frac{5}{8}, \right),$$
$$S_3 = (S_{3,1} \cup S_{3,2}) = \left(\frac{15}{16}, 1\right).$$

In regions of the phase space with a negative local Lyapunov exponent, the degradation of the map can occur due to the influence of both aforementioned factors. The impact of the phase space shrinking effect is significantly noticeable on the degradation at small number of iterations n. As n increases, this effect diminishes due to the thinning of the set, as fewer and fewer points will be sufficiently close to "converge" into one.

VII. CONCLUSION

In this paper, we focused on the logistic equation and its behaviour under floating-point arithmetic. Our study aimed to find out how limits of number precision, rounding errors and the order of arithmetic operations influence the periodicity of iterations and the overall degradation of nonlinear dynamical systems when implemented in software.

The analysis revealed that floating-point arithmetic as well as fixed-point significantly affects the periodicity of the logistic equation's iterations, introducing errors that can alter the expected dynamical behaviour. It is found that the maximal cycle length of logistic map with floating-point arithmetic does not exceed tens of millions of iterations. Furthermore, the sequence in which arithmetic operations are performed was shown to play a crucial role in the system's stability, indicating that changes in operation order can lead to different outcomes in chaotic systems.

In addition, we examined the properties of weakly coupled logistic maps, highlighting how floating-point arithmetic can affect their interactions and potentially lead to increase of cycles of chaotic map. The study also compared the efficiency of various arithmetic standards, underscoring that no more than 2^{-3} part of number space is used to represent chaotic timeseries.

Finally, the research delved into the internal mechanisms behind the degradation of the logistic equation's dynamics, offering a detailed explanation of how precision limitations and rounding errors propagate through the system. These findings contribute to a deeper understanding of the challenges faced when implementing chaotic systems in computational environments, providing insights that are crucial for the accurate modelling and simulation of nonlinear dynamics.

AUTHOR CONTRIBUTIONS

O.K., S.H., V.I., R.P. – conceptualization, methodology, investigation, writing (original draft preparation), writing (review and editing).

COMPETING INTERESTS

The authors declare that they have no conflict of interest.

ACKNOWLEDGMENT

The authors acknowledge the support from NFDU project №2023.04/0150 "Development of mobile radiowave source positioning and power measuring and visualising system".

REFERENCES

[1] F. Sun, Z. Lv, and C. Wang, "Pseudo-random number generation based on spatial chaotic map of Logistic type and its cryptographic application," *International Journal of Modern Physics C*, vol. 35, no. 1, pp. 1-17, Jan. 2024.

[2] H. Zhao, S. Xie, and J. Zhang, "Fast image encryption based on new cascade chaotic system and Rubik's cube strategy," *Multimedia Tools and Applications*, vol. 83, no. 9, pp. 1-15, 2024.

[3] Mihailescu, M.I., Nita, S.L. Chaos-based Cryptography. In: Pro *Cryptography and Cryptanalysis with C++23*. Apress, Berkeley, CA, 2023.

[4] A. Semenov, O. Osadchuk, O. Semenova, O. Bisikalo, O. Vasilevskyi and O. Voznyak, "Signal Statistic and Informational Parameters of Deterministic Chaos Transistor Oscillators for Infocommunication Systems," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 730-734

[5] Mykola Kushnir, Hryhorii Kosovan, i Petro Kroialo, "Investigation of properties of chaotic generators of pseudo-random sequences constructed using fuzzy logic", *IKKT*, vol. 1, p. 63-72, Jan. 2022.

[6] O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi "Testing timeseries ring-coupled map generated by on FPGA", *Telecommunication and Informative Technologies* – 2016. – №4(53). – C. 24-29.

[7] S. Bhattacharjee, H. Sharma, T. Choudhury, and A. M. Abdelmoniem, "Leveraging chaos for enhancing encryption and compression in large cloud data transfers", *The Journal of Supercomputing*, Feb. 2024.

[8] 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.

[9] O. Krulikovskyi and S. Haliuk, "Periodicity of Timeseries Generated by Logistic Map. Part I", *SISIOT*, vol. 1, no. 2, p. 02010, Dec. 2023.

[10] C. Fan, Q. Ding, "Effects of Limited Computational Precision on the Discrete Chaotic Sequences and the Design of Related Solutions", *Complexity*, 2019, 3510985, 2019.

[11] C. L. Fan and Q. Ding, "Analyzing the period distribution of digital chaos with graph theory," *Physica Scripta*, vol. 96, no. 8, p. 085212, May 2021.

[12] L.-C. Cao, Y.-L. Luo, S.-H. Qiu, and J.-X. Liu, "A perturbation method to the tent map based on Lyapunov exponent and its application," *Chinese Physics B*, vol. 24, no. 10, p. 100501, Sep. 2015.

[13] J. Zheng, H. Hu, and X. Xia, "Applications of symbolic dynamics in counteracting the dynamical degradation of digital chaos," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1535–1546, Jul. 2018.

[14] D. Goldberg, "What every computer scientist should know about floating-point arithmetic," *ACM Computing Surveys*, vol. 23, no. 1, pp. 5–48, Mar. 1991.

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: 0000-0001-5995-6857

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, signal processing and software development. Author of more than 40 publications.

ORCID ID: 0000-0003-3836-2675

Viktor Ivashko

Assistant at the Computer Sciences Department of Chernivtsi National University. His research field covers computer modeling of stochastic processes in physical systems. Author of more than 18 publications.

ORCID ID: 0000-0002-9339-4648

Ruslan Politanskyi

Received a Ph.D. in solid state physics from Yuriy Fedkovych Chernivtsi National University. Received a Dr. of Eng. Science in Telecommunication from National University «Lviv Polytechnic». His research interests include signal processing, coding theory, pseudorandom sequence systems with chaotic dynamics, physical principles of processes for information coding, distribution and transferring.

ORCID ID: 0000-0003-0015-7123

Періодичність цифрової реалізації логістичного рівняння. Частина II

Олег Круліковський[1,2,3], Сергій Галюк[1,*], Віктор Івашко[4], Руслан Політанський[1]

[1]Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна
[2]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
[3]Факультет електротехніки та комп'ютерних наук, Сучавський університет імені Стефана чел Маре, 720229 Сучава, Румунія
[4]Кафедра комп'ютерних наук, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: s.haliuk@chnu.edu.ua)

АНОТАЦІЯ У статті розглянуто вплив обмеженої точності обчислень на динаміку дискретних хаотичних систем, які використовуються в криптографії. Основна увага приділяється тому, як арифметика з рухомою комою впливає на періодичність і деградацію хаотичних часових рядів. Показано, що обмеження точності обчислень можуть призвести до спрощення динаміки хаотичних систем, зокрема, до зменшення кількості можливих станів системи та, відповідно, до зниження надійності хаотичного шифрування. Зокрема, дослідження виявило, що використання арифметики з рухомою комою зумовлює деградацію динаміки хаотичної системи перетворюючи її на регулярну, або призводить до колапсу, коли виходом є постійне значення. Причиною цього є поєднання властивостей перемішування та стиснення фазового простору при обмеженій множині можливих значень стану системи, якою оперує обчислювальний пристрій: якщо різниця між траєкторіями системи на деякій ітерації стає меншою за машинний нуль, то такі траєкторії збігаються в одну. На прикладі логістичного відображення показано, що різні початкові умови та параметри призводять до виникнення циклів різної довжини. Аналогічно до арифметики з фіксованою комою, спостерігається переважання одного чи кількох циклів до яких прямує система з абсолютної більшості початкових умов. Для арифметики з рухомою комою встановлено, що максимальна довжина циклів не перевищує кілька десятків мільйонів ітерацій. Дослідження також показало, що порядок виконання арифметичних операцій і вибір методів з'єднання окремих хаотичних відображень у систему значно впливають на її динаміку. Система слабо з'єднаних логістичних рівнянь характеризується суттєвим зростанням періоду повторення. Проте такий спосіб збільшення тривалості циклів не гарантує відсутність коротких циклів чи колапсу системи. Крім того, неправильний вибір коефіцієнта з'єднання може призвести до синхронізації з'єднаних систем, коли зростання періоду у середньому відсутнє.

КЛЮЧОВІ СЛОВА періодичність хаосу, хаотичні послідовності, логістичне відображення.