DOI 10.31891/2307-5732-2019-279-6-110-115
УДК 621.391

О.В. КРУЛІКОВСЬКИЙ, С.Д. ГАЛЮК
Чернівецький національний університет імені Юрія Федьковича

ЦИКЛІЧНІСТЬ ПОСЛІДОВНОСТЕЙ, ГЕНЕРОВАНИХ МЕМРИСТОРНОЮ ХАОТИЧНОЮ СИСТЕМОЮ

В роботі на прикладі математичної моделі мемристорного генератора хаотичних коливань вивчається доцільність застосування методів чисельного рішення диференційних рівнянь високої точності в криптографічних алгоритмах. Використовуючи Simulink-моделі хаотичної системи і арифметику з фіксованою комою досліджено періодичність реалізацій отриманих за допомогою методів Ейлера та Рунге-Кутти четвертого порядку. Показано, що з врахуванням часової складності виконання операцій при програмній і програмно-апаратній реалізації неперервних хаотичних систем доцільно користуватися методом Ейлера.

Ключові слова: хаотична система, мемристорна структура, періодичність, метод Ейлера, метод Рунге-Кутти, хаотична криптографія.

O.V. KRULIKOVSKYI, S.D. HALIUK
Yuriy Fedkovych Chernivtsi National University

CYCLICITY OF TIME SERIES GENERATED BY MEMRISTOR BASED CHAOTIC CIRCUIT

In the paper the solutions periodicity of the mathematical model of the memristor chaotic oscillator and expediency of application different methods of high precision numerical solution of differential equations in cryptographic algorithms is studied. Based on Lyapunov exponent theory the dynamic of chaotic system and its dependencies from system parameters is explored. There are several ranges of system parameters where the largest Lyapunov exponent is greater zero and memeristor system has chaotic modes. The transition from continuous system to discretized model is discussed. Using probability density and atractors it is shown saving of properties of chaotic regimes for different methods of numerical modelling. The periodicity of timeseries obtained by Euler and Runge-Kutta methods is studied by Simulink-model of chaotic systems and fixed-point arithmetic. For timeseries of discrete chaotic system the average period is computed. When timestep is equal $\Delta t = 0,0005 - 0,02$ *and fixed-point arithmetic Q8.16 average period is about* $10^6 \div 2*10^6$ *iterations. If discrete-time series save the original chaotic modes of continuous system, then average period do not depend from timestep of discrete model and computation complexity. It is shown that taking into consideration the complexity of computation for hardware implementation of continuous chaotic systems is advisable to use the Euler method. If timestep close to precision of computation, after several tens iterations collapse of chaos of discrete-time systems is appear with a one-step length period.*

Keywords: chaotic system, memristor system, periodicity, Euler method, Runge-Kutta method, cryptography.

Вступ

Починаючи із другої половини 80-х років XX ст. детерміновані динамічні системи є актуальним напрямом наукових досліджень [1–5] в системах технічного захисту інформації. Хаотичні системи неперервного часу реалізовуються на базі аналогових схем, при цьому спектральні і статистичні характеристики сигналів визначатимуться параметрами схеми (номіналами лінійних і нелінійних елементів). Для побудови системи зв'язку необхідно використовувати два ідентичних генератори. Однак внаслідок впливу теплових шумів та технологічних обмежень на прецизійність елементів електричних кіл виникає проблема встановлення стійкої завадозахищеної синхронізації. Синхронізація таких генераторів може бути досягнута тільки тоді, коли вони будуть близькими за значенням параметрів розкид яких не повинен перевищувати 1 %. Реалізація ідентичних генераторів можлива в інтегральному виконані з лазерною підгонкою на інтегральній мікросхемі [6]. При виході з ладу одного з генераторів заміні підлягатимуть обидва.

Технологічна складність забезпечення ідентичності рознесених генераторів хаосу обмежує їх застосування в системах зв'язку. Одним із шляхів вирішення проблеми забезпечення прецизійності елементної бази є програмно-апаратна реалізація генераторів хаотичних коливань з використанням ПЛІС (програмованих логічних інтегральних схем). Однак перехід до скінченої множини дискретних станів призводить до деградації динаміки і циклічності отриманих чисельними методами хаотичних рядів [7]. При переході від неперервної до дискретної моделі розв'язки системи зберігатимуть властивості фазового простору, розмірності, ергодичності, спектру та ін., проте будуть циклічними. В [8] показано, що довжина циклів значно менша потужності множини можливих станів системи і залежить від кореляційної розмірності та точності обчислень. Різні початкові умови призводять до однакових циклів, що обмежує їх кількість. Для окремих систем можливе явище колапсу хаосу, яке полягає у встановленні циклу періодом в одну ітерацію [9].

В [10, 11] запропоновано методи генерування псевдовипадкових послідовностей на базі математичних моделей хаотичних систем із неперервним часом. Однак в даних роботах питання періодичності розв'язків та їх залежність від обраного чисельного методу інтегрування та точності обчислень не розглядається, хоча є важливим при побудові криптографічних методів захисту інформації.

Метою роботи є аналіз періодичності розв'язків математичної моделі хаотичної системи на базі мемристора [12, 13], використання якого забезпечує просту структуру електричного кола, що демонструє складну динаміку при заданих параметрах. Для досліджень обрано чисельні методи Ейлера та Рунге-Кутти 4-го порядку.

Опис математичної моделі

Мемристор є одним з останніх досягнень розробки та виготовлення нелінійних елементів з використанням інтегральної технології і може бути виготовлений з використанням органічних та

неорганічних матеріалів. Нелінійна динаміка мемристора може бути використана для реалізації малопотужних захищених систем зв'язку. Один з найпростіших генераторів хаотичних коливань на базі мемристора описаний в роботі в [13]. Схема складається з трьох послідовно з'єднаних елементів: індуктивності, конденсатора та мемристорного елемента (рис. 1).

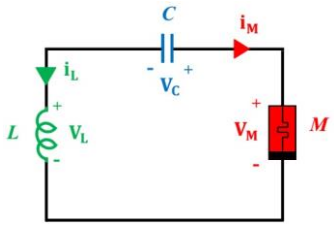


Рис. 1. Електрична схема хаотичної системи на базі мемристора

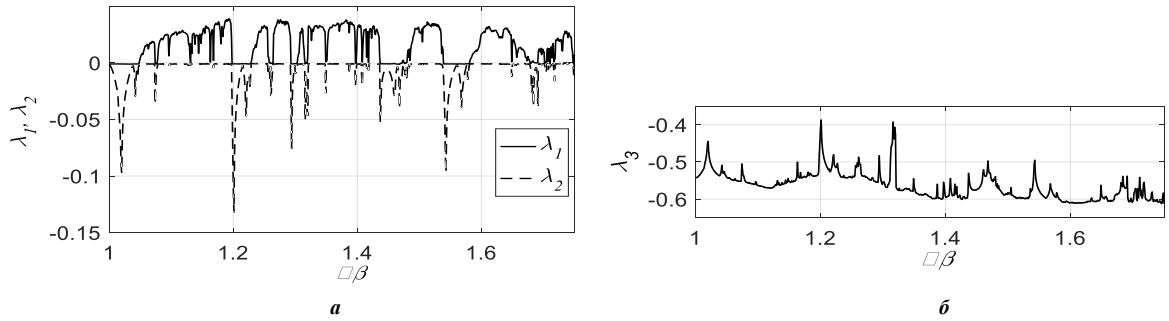
Використана нами модель мемристора є моделлю узагальненого мемристорного пристрою [14] характеристики якого не відповідають характеристикам ідеального мемристора введеного в [15]. Нелінійна характеристика мемристора описується рівнянням:

$$\begin{cases} V_M = \beta(x^2-1)i_M \\ \dot{x} = i_M - \alpha x - i_M x \end{cases} \tag{1}$$

Динаміка електричного кола (рис. 1) описується системою диференційних рівнянь [4]:

$$\begin{cases} \dot{x} = y/C, \\ \dot{y} = -1/L\left[x + \beta(z^2-1)y\right], \\ \dot{z} = -y - \alpha z + yz, \end{cases} \tag{2}$$

де значення параметрів для хаотичного режиму $C = 1\ Ф$, $L = 3\ Гн$. Критерієм хаотичної поведінки є **додатне** значення старшого показника Ляпунова. Визначена за допомогою методу Бенеттина, діаграма показників Ляпунова для системи (2) наведена на рис 2. При значеннях параметру $\beta \in [1,1,7]$ в системі мають місце періодичні $(\lambda_1 = 0)$ і хаотичні $(\lambda_1 > 0)$ режими.



а *б*

Рис. 2. Залежність показників Ляпунова від параметру β при α = 0,6

Дослідження проводилися для значень параметрів $\beta = 1,5$ та $\alpha = 0,6$. При $\beta = 1,5, L = 3Гн$, $\alpha = 0,6$ з рис. 2*а*. випливає, що система характеризується хаотичною поведінкою, оскільки найбільший показник Ляпунова є додатнім, а сума показників є від'ємною.

Моделювання розв'язків

Розв'язки чисельними методами диференційних рівнянь відрізняються ступенем їх наближення до точних розв'язків системи. Розв'язки отримані при моделюванні хаотичних систем з врахуванням їх чутливості до як завгодно малих відхилень початкових умов на великих проміжках часу значно відрізняються від точних розв'язків. Метою моделювання нелінійної системи є отримання реалізацій, що зберігають статистичні властивості ідеальних систем. Більшість хаотичних систем є ергодичними, тому їх дослідження можна проводити на основі однієї реалізації. Проте розв'язки, отримані методом чисельного моделювання, повинні зберігати поведінку хаотичного атрактора.

Суть чисельних методів полягає у представленні системи диференційних рівнянь у вигляді рекурентної залежності та розрахунку послідовності точок на траєкторії у дискретні моменти часу з кроком Δt. Найбільш простим за обчислювальною складністю є метод Ейлера, в якому зв'язок між сусідніми точками траєкторій системи (2) описується наступною залежністю

$$\begin{cases} x_{n+1} = f_1(t_n, y_n)\Delta t + x_n, \\ y_{n+1} = f_2(t_n, x_n, y_n, z_n)\Delta t + y_n, \\ z_{n+1} = f_3(t_n, y_n, z_n)\Delta t + z_n, \end{cases} \tag{3}$$

де

$$\begin{cases} f_1 = \dfrac{y_n}{C}, \\ f_2 = -\dfrac{1}{L}\left[x_n + \beta(z_n^2 - 1)y_n\right], \\ f_3 = -y_n - \alpha z_n + y_n z_n. \end{cases} \quad (4)$$

Широкого застосування набув метод Рунге-Кутти четвертого порядку, що характеризується вищою точністю розрахунків. Згідно з цим методом залежність між станами системи у послідовні дискретні моменти часу є наступною:

$$\begin{cases} x_{n+1} = x_n + \dfrac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4), \\ y_{n+1} = y_n + \dfrac{1}{6}(m_1 + 2m_2 + 2m_3 + m_4), \\ z_{n+1} = z_n + \dfrac{1}{6}(l_1 + 2l_2 + 2l_3 + l_4), \end{cases} \quad (5)$$

де

$$k_1 = f_1(t_n, y_n)\Delta t,\ m_1 = f_2(t_n, x_n, y_n, z_n)\Delta t, l_1 = f_3(t_n, y_n, z_n)\Delta t,$$

$$k_2 = f_1(t_n + \frac{\Delta t}{2}, y_n + \frac{m_1}{2})\Delta t,\ m_2 = f_2(t_n + \frac{\Delta t}{2}, x_n + \frac{k_1}{2}, y_n + \frac{m_1}{2}, z_n + \frac{l_1}{2})\Delta t,$$

$$l_2 = f_3(t_n + \frac{\Delta t}{2}, y_n + \frac{m_1}{2}, z_n + \frac{l_1}{2})\Delta t,$$

$$k_3 = f_1(t_n + \frac{\Delta t}{2}, y_n + \frac{m_2}{2})\Delta t,\ m_3 = f_2(t_n + \frac{\Delta t}{2}, x_n + \frac{k_2}{2}, y_n + \frac{m_2}{2}, z_n + \frac{l_2}{2})\Delta t,$$

$$l_3 = f_3(t_n + \frac{\Delta t}{2}, y_n + \frac{m_2}{2}, z_n + \frac{l_2}{2})\Delta t,$$

$$k_4 = f_1(t_n + \Delta t, y_n + m_3)\Delta t,\ m_4 = f_2(t_n + \Delta t, x_n + k_3, y_n + m_3, z_n + l_3)\Delta t,$$

$$l_4 = f_3(t_n + \Delta t, y_n + m_3, z_n + l_3)\Delta t.$$

Значення функцій f_1, f_2, f_3 розраховуються згідно з (4). Приклади портретів фазових атракторів, отриманих під час застосування методу Ейлера та Рунге-Кутти, наведені на рис. 3.

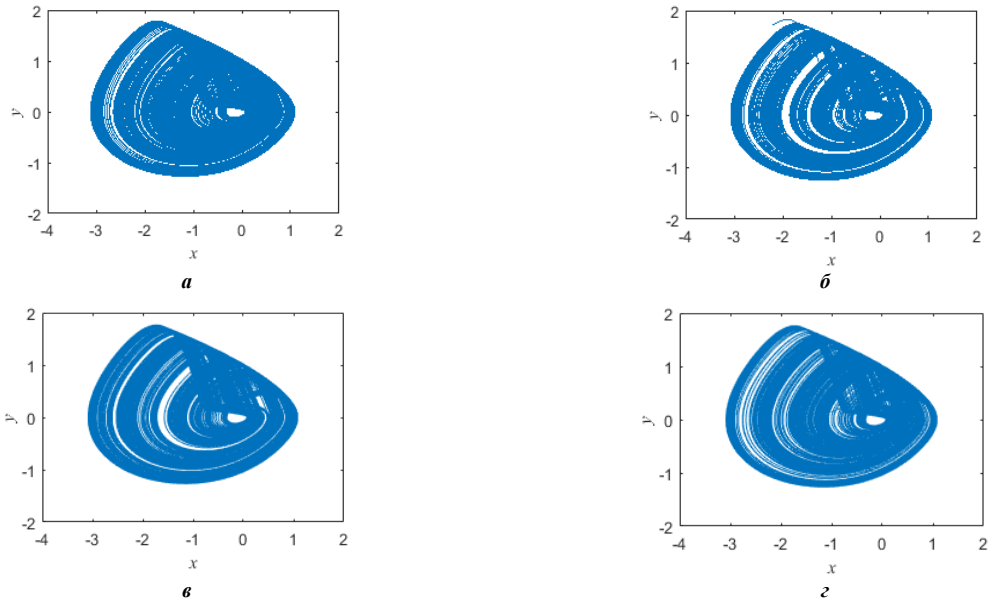


Рис. 3. Хаотичний атрактор системи (2) при $\Delta t = 0,001$ розрахунку методом Ейлера – *а, в*; Рунге-Кутти четвертого порядку – *б, г*. Рис. *а* і *б* отримані з використанням арифметики Q8.16, а *в* і *г* – з використанням арифметики Q8.24

Всі атрактори зберігають форму, характеризуються однаковою структурою з однаковим розмахом реалізацій незалежно від точності розрахунків.

Гістограми розподілу змінної *x* для різної точності та методів розрахунку є подібними (рис. 4), що вказує на збереження фрактальних розмірностей системи.

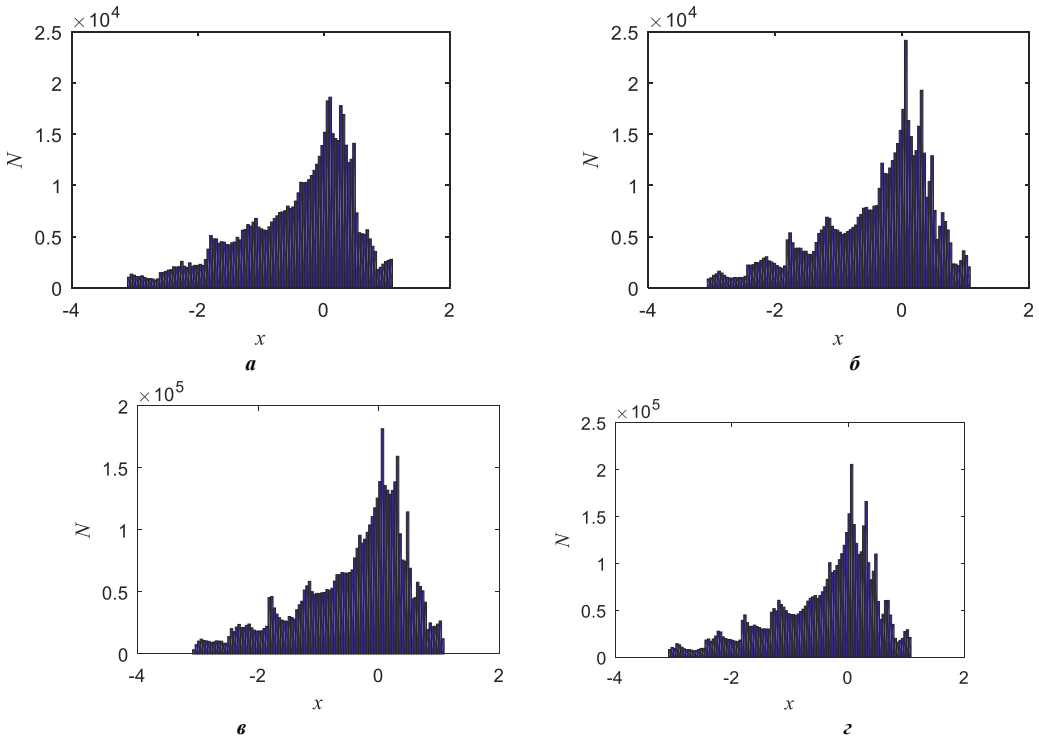


Рис. 4. Гістограми розподілу реалізацій змінної *x* системи (2) при $\Delta t = 0,001$ розрахунку методом Ейлера – *а, в*; Рунге-Кутти четвертого порядку – *б, г*. Рис. *а* і *б* отримані для арифметики Q8.16, *в* і *г* – для арифметики Q8.24

З аналізу залежностей, представлених на рис. 3 і рис. 4, слідує висновок про однакову результативність застосування методів Ейлера та Рунге-Кутти з метою збереження псевдохаотичних характеристик розв'язками дискретизованої системи. Обидва методи дають змогу отримувати хаотичні ряди, які зберігають властивості сигналів оригінальної недискретизованої системи (2).

Періодичність та колапс

Для проведення дослідження розроблено Simulink-моделі системи (2), що реалізують методи Ейлера та Рунге-Кутти четвертого порядку. Всі розрахунки здійснено в арифметиці з фіксованою комою Q8.16 з точністю 24 біта, з яких 16 біт відведено на дробову частину. Приклад реалізації (2) за допомогою методу Ейлера наведено на рис. 5. У схемі використано стандартні засоби Simulink, операція інтегрування здійснюється блоками "Discrete-Time integrator". Під час розрахунків проводилося заокруглення до меншого значення.

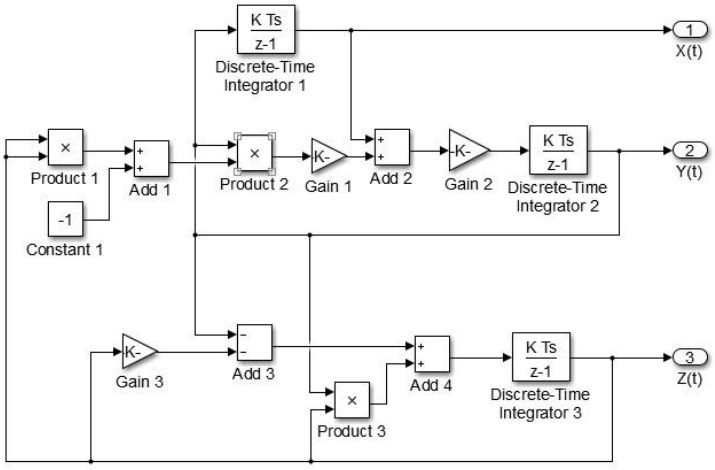


Рис. 5. Simulink-модель хаотичної системи для розрахунків методом Ейлера

Для 25 значень випадкових початкових умов та 25 значень параметрів системи в околі $\beta = 1,5$ та $\alpha = 0,6$ залежність середнього періоду, що встановлюється внаслідок деградації хаотичної системи, від кроку по часу наведено на рис. 6.

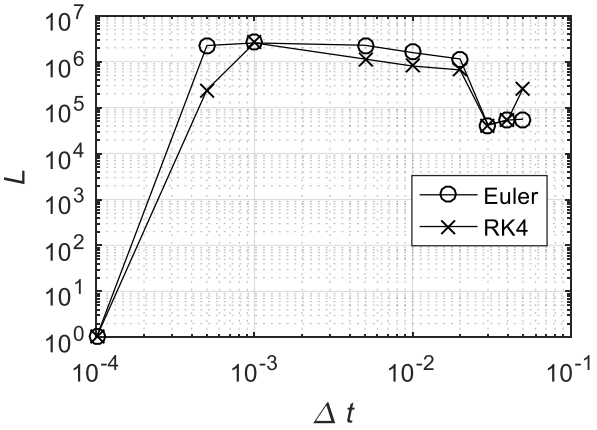


Рис. 6. Залежність середнього періоду від кроку по часу для методу Ейлера та Рунге-Кутти четвертого порядку

З рис. 6. випливає, що збільшення складності розрахунків не призводить до збільшення тривалості періоду повторення реалізацій системи. Середня тривалість циклу знаходиться в межах $10^6 \div 2 \cdot 10^6$ ітерацій і не залежить від кроку дискретизації при $\Delta t = 0,0005 \div 0,02$. При $\Delta t = 0,0001$ для обох методів розрахунку спостерігається колапс, обумовлений втратою точності розрахунків внаслідок заокруглення чисел. Після перехідного процесу тривалістю в кілька десятків ітерацій, в системі встановлюється цикл довжиною одну ітерацію (рис. 7).

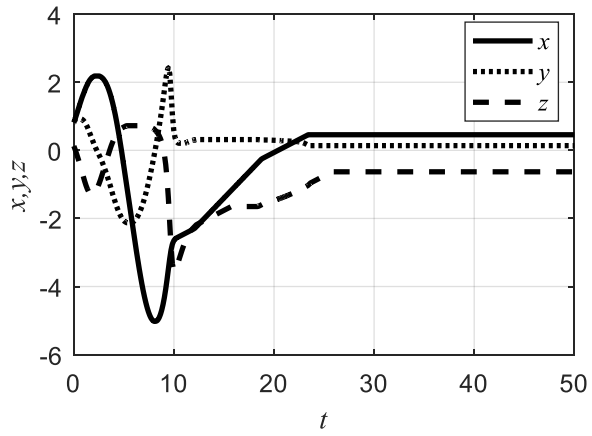


Рис. 7. Колапс хаотичної системи при Δt = 0,0001

У випадку зростання інтервалу дискретизації, при $\Delta t \geq 0,03$ середнє значення періоду повторення зменшується до $\sim 5 \cdot 10^4$, що може бути обумовлено зміною структури системи внаслідок лінеаризації на великому проміжку часу.

Висновки

В роботі за допомогою чисельних методів Ейлера та Рунге-Кутти досліджено математичну модель електричного кола з хаотичною поведінкою з використанням арифметики з фіксованою комою. Проведено порівняльний аналіз ефективності чисельних методів розв'язку нелінійних диференційних рівнянь, що описують хаотичні системи. Показано, що застосування методу Рунги-Кутти не призводить до збільшення періоду повторення псевдохаотичних рядів. Встановлено, що для побудови генераторів псевдовипадкових послідовностей достатньо використовувати прості методи рішення диференційних рівнянь, зокрема, метод Ейлера.

Література

1. Pecora L. M. Synchronization in chaotic systems / L. M. Pecora, T.L. Carroll // Phys. Rev. Lett. – 1990. – Vol. 64. № 8. – P. 821–824.

2. Птицын Н. Приложение теории детерминированного хаоса в криптографии / Н. Птицын. – Москва : МГТУ им. Н. Э. Баумана, 2002. – 80 с.

3. Kocarev L. Chaos-Based Cryptography Theory, Algorithms and Applications / Ljupco Kocarev, S. Lian. – Berlin : Springer-Verlag Berlin Heidelberg, 2011. – 397 p.

4. Галюк С.Д. Порівняльний аналіз двомірних відображень для перестановок пікселів / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету. Технічні науки. – 2017. – № 1(245). – С. 214–220.

5. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Сучасний захист інформації. – 2016. – № 2. – С. 69–77.

6. Keuninckx L. Encryption key distribution via chaos synchronization / Keuninckx Lars, Soriano Miguel C., Fischer Ingo, Mirasso Claudio R., Nguimdo Romain M., Van der Sande Guy // Scientific Reports. – 2017. – Vol. 7.

7. Шахтарин Б.И. Генераторы хаотических колебаний / Б.И. Шахтарин, П.И. Кобылкина, Ю.А. Сидоркина, А.В. Кондратьев, С.В. Митин. – Москва : Галилеос АРВ, 2007. – 247 с.

8. Bernard H. Probability Distributions Related to Random Mappings / Bernard Harris // Ann. Math. Statist. – 1960. – Volume 31, Number 4. – P. 1045–1062.

9. Yuan G. Collapsing of chaos in one dimensional maps / G. Yuan, J. A. Yorke // Physica D: Nonlinear Phenomena. – 2000. – № 136. – P. 18–30.

10. Mansingka A.S. Fully digital jerk-based chaotic oscillators for high throughput pseudo-random number generators up to 8.77 Gbits/s / A.S. Mansingka, M. Affan Zidan, M.L. Barakat, A.G. Radwan, K.N. Salama // Microelectron. Jour. –2013. – Vol. 44, Issue 9. – P. 744–752.

11. Lahcene Merah A Pseudo Random Number Generator Based on the Chaotic System of Chua's Circuit, and its Real Time FPGA Implementation / Lahcene Merah, Adda Ali-Pacha, Naima Hadj Said, Mustafa Mamat // Applied Mathematical Scien. – 2013. – Vol. 7, no. 55. – P. 2719–2734.

12. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, 18–20 April 2016, IEEE.

13. Muthuswamy B. Simplest chaotic circuit / Bharathwaj Muthuswamy, Leon O. Chua // Int. J. of Bif. and Chaos. – 2010. – Vol. 20, № 5. – P. 1567–1580.

14. Chua L.O. Memristive devices and systems / L.O. Chua, S.M. Kang // Proc. IEEE. – 1976. – № 64. – P. 209–223.

15. Chua L.O. Memristor – The missing circuit element / Chua L.O. // IEEE Trans. Circuit Th. – 1971. – CT–18. – P. 507–519.

References

1. Pecora L. M. Synchronization in chaotic systems / L. M. Pecora, T.L. Carroll // Phys. Rev. Lett. – 1990. – Vol. 64. № 8. – P. 821–824.

2. Pticyn N. Prilozhenie teorii determinirovannogo haosa v kriptografii / N. Pticyn. – Moskva : MGTU im. N. E. Baumana, 2002. – 80 s.

3. Kocarev L. Chaos-Based Cryptography Theory, Algorithms and Applications / Ljupco Kocarev, S. Lian. – Berlin : Springer-Verlag Berlin Heidelberg, 2011. – 397 p.

4. Haliuk S.D. Porivnialnyi analiz dvomirnykh vidobrazhen dlia perestanovok pikseliv / S.D. Haliuk, O.V. Krulikovskyi, L.F. Politanskyi // Herald of Khmelnytskyi National University. – 2017. – № 1(245). – C. 214–220.

5. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Cuchasnyi zakhyst informatsii. – 2016. – № 2. – C. 69–77.

6. Keuninckx L. Encryption key distribution via chaos synchronization / Keuninckx Lars, Soriano Miguel C., Fischer Ingo, Mirasso Claudio R., Nguimdo Romain M., Van der Sande Guy // Scientific Reports. – 2017. – Vol. 7.

7. Shahtarin B.I. Generatory haoticheskih kolebanij / B.I. Shahtarin, P.I. Kobylkina, Yu.A. Sidorkina, A.V. Kondratev, S.V. Mitin. – Moskva : Galileos ARV, 2007. – 247 s.

8. Bernard H. Probability Distributions Related to Random Mappings / Bernard Harris // Ann. Math. Statist. – 1960. – Volume 31, Number 4. – R. 1045–1062.

9. Yuan G. Collapsing of chaos in one dimensional maps / G. Yuan, J. A. Yorke // Physica D: Nonlinear Phenomena. – 2000. – № 136. – R. 18–30.

10. Mansingka A.S. Fully digital jerk-based chaotic oscillators for high throughput pseudo-random number generators up to 8.77 Gbits/s / A.S. Mansingka, M. Affan Zidan, M.L. Barakat, A.G. Radwan, K.N. Salama // Microelectron. Jour. –2013. – Vol. 44, Issue 9. – R. 744–752.

11. Lahcene Merah A Pseudo Random Number Generator Based on the Chaotic System of Chua's Circuit, and its Real Time FPGA Implementation / Lahcene Merah, Adda Ali-Pacha, Naima Hadj Said, Mustafa Mamat // Applied Mathematical Scien. – 2013. – Vol. 7, no. 55. – R. 2719–2734.

12. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, 18–20 April 2016, IEEE.

13. Muthuswamy B. Simplest chaotic circuit / Bharathwaj Muthuswamy, Leon O. Chua // Int. J. of Bif. and Chaos. – 2010. – Vol. 20, № 5. – R. 1567–1580.

14. Chua L.O. Memristive devices and systems / L.O. Chua, S.M. Kang // Proc. IEEE. – 1976. – № 64. – R. 209–223.

15. Chua L.O. Memristor – The missing circuit element / Chua L.O. // IEEE Trans. Circuit Th. – 1971. – CT–18. – R. 507–519.

Рецензія/Peer review : 24.12.2019 р. Надрукована/Printed : 02.01.2020
Рецензент: д. ф.-м. н., проф. Сльотов М.М.