УДК 004.056.55

Круліковський О. В., Галюк С. Д., Політанський Л. Ф.
Чернівецький національний університет імені Юрія Федьковича

ОСОБЛИВОСТІ ВИБОРУ ХАОТИЧНИХ СИСТЕМ ДЛЯ ПОБУДОВИ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

В роботі виокремлено базові критерії, яким повинні відповідати хаотичні системи для їх застосування при побудові криптографічних додатків. Показано, що для правильної оцінки потужності множини ключів, необхідно уникати значень параметрів за яких мають місце нехаотичні режими, що можна досягнути використанням багатовимірних відображень. Вказано шляхи збільшення періоду хаотичних систем при їх програмній і програмно-апаратній реалізації в умовах обмеженої прецизійності обчислень. Для багатомірних варіантів сімейств відображень Лоці та гіперхаотичної системи Тратаса встановлено існування хаотичних режимів неперервних за параметрами керування.

Ключові слова – хаотичні системи, простір ключів, рівномірний розподіл, періодичність розв'язків.

Krulikovskyi O. V. , Haliuk S. D. , Politanskyi L. F. Features of choosing the chaotic systems for constructing generators of pseudo-random numbers. In the paper are emphasized the basic criteria which the chaotic systems must pass for their use in the constructing of cryptographic applications. On example of logistic map it is shown, that to estimate the power of the set of keys properly, is necessary to avoid parameter values for which nonchaotic modes exist, what can be achieved by using the multidimensional maps. It is shown, that for software implementation of one-dimensional chaotic maps are observed collapse of chaos and short lengths of cycles in dependence from parameters and precision of calculations. It is noted methods of increasing the period of chaotic systems at their software and software-hardware implementation in conditions of limited precision calculations. It is shown that need use the ring-coupled maps to avoid collapse of chaos and short lengths of time series. For multidimensional variants of Lozi families maps and Tratas hyperchaotic system is determined the existence of chaotic modes continuous in control parameters.

Keywords – chaos, key space, continuous bifurcation diagram, uniform distribution, periodicity of solutions, precision of calculations, PRNG, rind-coupled maps.

1. Вступ. Починаючи з другої половини 80-х років XX ст. системи цифрового зв'язку на базі детермінованого хаосу є активним полем наукових досліджень, що обумовлено необхідністю вирішення багатогранної складності питань інформаційної безпеки, які виникли внаслідок швидкого розвитку і тотального впровадження новітніх технологій [1-3]. Як відомо найбільш ефективним засобом для захисту даних є їх криптографічне зашифрування. Постійне збільшення можливостей ЕОМ призводить до систематичного підвищення вимог до криптографічних додатків. Ці обставини вимагають розвитку і дослідження нових областей в криптології. Детерміновані хаотичні системи за типом генерованих коливань поділяють на два класи: системи з дискретним і неперервним часом [4]. Системи з дискретним часом описуються рекурсивними рівняннями, а системи із неперервним часом – нелінійними диференційними рівняннями (цілого або дробового порядку) [5]. Неперервні хаотичні сигнали генеруються аналоговими схемами, а їх спектральні і статистичні характеристики визначаються параметрами схеми (номіналами лінійних і нелінійних елементів).

Аналогові генератори дискретних сигналів є неавтономними, що працюють під дією тактового сигналу. Шириною спектру генерованих сигналів можна керувати шляхом зміни тактового сигналу. Однак, у силу впливу теплових шумів та технологічних обмежень на прецизійність елементів електричних кіл хаотичні системи набули популярності в якості генераторів випадкових чисел [6].

Іншим широким класом генераторів є генератори псевдовипадкових послідовностей (ГПВП) на базі програмних реалізацій детермінованих динамічних систем. Як відомо, ЕОМ характеризуються обмеженою точністю обчислень при розрахунках [7]. Тому програмно реалізовані детерміновані хаотичні системи з плином часу володітимуть властивістю циклічності, що обумовлено переходом від безмежної до скінченої множини.

Чисельно отримані розв'язки зберігатимуть спектр, розмірність, ергодичність та властивості атрактора [8]. Наприклад, довжина циклу одномірного хаотичного відображення (логістичного, кубічного, квадратичного або ін.), реалізованого на ПЛІС з фіксованою комою і точністю $n = 32$ двійкових розряди, матиме теоретично максимальний період 2^n.

З точки зору інформаційної безпеки висуваються вимоги до точності обчислень та статистичних властивостей ГПВП і простору ключів. На відміну від систем неперервного часу, що описуються диференційними рівняннями, пріоритетним для розробки криптографічних засобів є використання хаотичних систем дискретного часу, які оперують простими математичними операціями [9].

В роботі розглянуто критерії вибору дискретних хаотичних систем з метою побудови ГПВП на ПЛІС та обґрунтовано перехід до багатовимірних відображень на прикладі логістичного відображення. Показано, що не всі системи можуть бути використані в якості генератора часових рядів для формування ПВП, та підтверджено доцільність застосування хаотичних систем, що характеризуються суцільною діаграмою біфуркацій без вікон періодичності.

2. Періодичність хаосу. Загальновідомо, що детермінований хаос має місце в безмежному полі дійсних чисел [4]. При переході до програмної реалізації на базі ЕОМ внаслідок зменшення множини можливих станів хаотичні системи втрачають «хаотичність», а їх реалізації є псевдохаотичними і циклічними. Для мінімізації впливу цього фактору необхідно використовувати максимально можливу точність обчислень з урахуванням кросплатформеності та швидкодії. Неповна відповідність базових програмно-апаратних носіїв часто призводить до неможливості відтворення ідентичних псевдохаотичних реалізацій на різних платформах (різні ОС, мови програмування, компілятори, різні виробники ПЛІС).

При виконанні арифметичних операцій над дійсними числами у арифметиці з плаваючою комою має місце фактор різних значень похибки заокруглення, яка внаслідок чутливості нелінійних систем призводить до розбігання траєкторій для різних програмно-апаратних засобів та компіляторів. Використовуючи арифметику з фіксованою комою при заданому типі заокруглення можна уникнути різних похибок заокруглення [3]. Іншим варіантом є перехід до скінчених автоматів – аналогів хаотичних систем над скінченим кільцем Z_{p^k} (де p – просте число, а k – натуральне число) [10-11].

До переваги програмної реалізації арифметики з фіксованою комою варто віднести можливість рознесеного точного відтворення хаотичних сигналів (у тому числі з довільними часовими затримками), що відкриває можливості для розроблення криптографічних алгоритмів.

Для достатньо великого періоду повторення розв'язки хаотичної системи зберігатимуть розмірність, ергодичність та властивості справжнього атрактора. Це дає змогу досліджувати хаотичні системи шляхом їх моделювання. В [8] показано, що довжина циклу для логістичного рівняння становить $\sim 2^{10} \div 2^{16}$ для арифметики Q32.29, що значно менше теоретичного максимуму в 2^{32} ітерацій. Кількість циклів при одному значенні параметру є обмеженою, внаслідок того що велика кількість траєкторій, формованих при різних початкових умовах, після закінчення перехідного процесу виходять на однакові дискретні періодичні орбіти. Внаслідок циклічності псевдохаотичної послідовності об'єм інформації, що підлягає за шифруванню та простір ключів методу є обмеженими.

Вирішення проблеми усунення повторюваності псевдохаосу можливе за рахунок збільшення середньої довжини циклу і тривалості перехідного процесу шляхом збільшення прецизійності обчислень та введення псевдовипадкових періодичних збурень а також переходом до багатовимірних систем.

Апаратне збільшення точності обчислень уможливлене при використанні дороговартісних пристроїв. Це є суттєвим стримуючим фактором, а програмна реалізація вимагає збільшення часових затрат.

Ефективність періодичних збурень залежить від властивостей системи, до якої вони застосовуються, характеру збурень та частоти їх дії. Для прикладу розглянемо логістичне відображення, що задається ітераційною залежністю:

$$x_{n+1} = r x_n \left(1 - x_n\right) \tag{1}$$

де r — параметр керування, n – номер ітерації, x_{n+1} – змінна, яка може приймати значення з діапазону [0; 1].

У випадку якщо тривалість циклу хаотичної системи становить одну ітерацію [12], збурення з періодом повторення більшим за середню тривалість перехідного процесу є недоцільні, оскільки вони призведуть до періодичного повторення частини однієї і тієї ж траєкторії. Реалізацію системи (1) у арифметиці Q12.9 під впливом випадкового періодичного збурення через кожні 50 ітерацій приведена на рис. 1. Із рис. 1 випливає, що дія збурення викликає короткий перехідний процес, після якого система колапсує або виходить на періодичну орбіту. Подібна ситуація матиме місце, у випадку, якщо середня тривалість циклів менша за період впливу збурення.

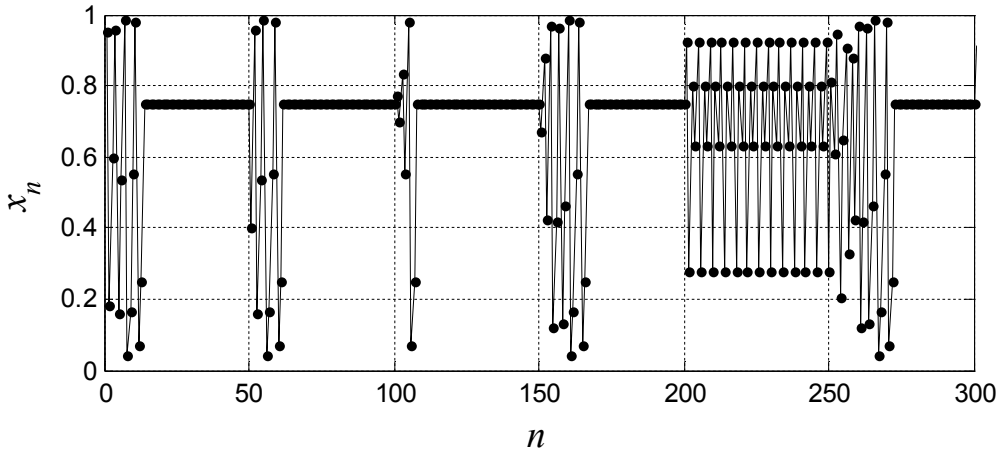


Рис. 1. Повторюваність колапсу при випадкових періодичних збуреннях через кожні 50 ітерацій

Використання багатовимірних систем є найбільш доцільним, оскільки кількість циклів повторення псевдохаосу, середня тривалість циклу та перехідного процесу перед виходом траєкторії на цикл пов'язані з кореляційною розмірністю d, як [13-14].

$$\left\langle L \right\rangle \sim \varepsilon^{-\frac{d}{2}}. \tag{2}$$

де $\left\langle L \right\rangle$ – позначає середнє значення.

Кореляційна розмірність не перевищує розмірності фазового простору хаотичної системи. Тому збільшення розмірності призведе до збільшення періоду повторення псевдохаотичної послідовності.

Варто зазначити, що у багатовимірних системах також можливі явища колапсу хаосу, проте середній час до виходу на одиничний цикл буде більшим в порівнянні з одно- та двовимірними хаотичними системами.

3. Розподіл хаотичних реалізацій. Особливістю хаотичних систем є різна частота відвідування їх траєкторіями різних областей фазового простору, що характеризується дробовими значеннями фрактальних розмірностей. Наслідком цього є нерівномірний розподіл значень послідовностей, генерованих такими системами.

Гістограма розподілу значень часових рядів, отриманих за допомогою (1) на (рис. 2.) є нерівномірною у всьому діапазоні значень параметру , що є небажаним для реалізації якісних криптографічних засобів. Безпосереднє використання розв'язків (1) як псевдовипадкових чисел, обумовлює їх нестійкість до статистичних атак [15].

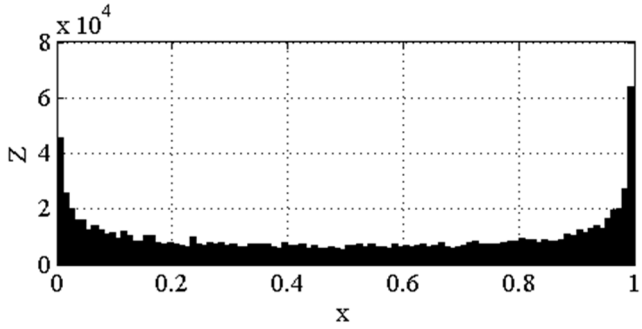


Рис. 2. Гістограма значень часових рядів генерованих (1) при $r = 3.999,\ n = 1000000.$

Найпростішим способом отримання за допомогою (1) псевдовипадкової послідовності є пороговий метод, згідно якому фазовий простір системи поділяється на дві незалежні області, що відповідають двійковим символам «0» або «1»:

$$X(n) = \begin{cases} 0, & x_n \le x_П \\ 1, & x_n > x_П \end{cases}, \tag{3}$$

де $x_П$ – порогове значення.

Отримана згідно (2) ПВП $X(n)$ є грубою оцінкою хаотичної траєкторії . Недоліком порогового методу є залежність статистичних характеристик послідовності від вибору порогового значення $x_П$. В [16] пропонується вибирати $x_П = 0.5$. Проте в роботах [17] показано, що внаслідок нерівності розподілу $x(n)$ такий вибір порогу $x_П$ не може забезпечити отримання збалансованих послідовностей. На рис. 3 приведено залежність відсотка «1» у послідовності, отриманій згідно (1) і (2) від значення параметру керування . Як бачимо, частки символів «0» і «1» при виборі порогу $x_П = 0.5$ значно різняться, що вказує на незбалансованість послідовності $X(n)$.

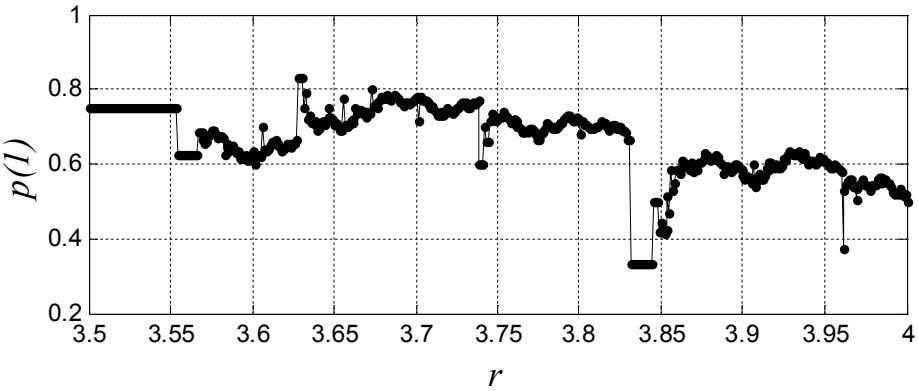


Рис. 3. Залежність ймовірності отримати символ «1» пороговим методом при $x_П = 0.5$ від параметру керування *r*.

Усунути недолік порогового методу можна динамічним вибором порогу, як медіани розподілу при заданому значені параметру керування (рис. 4).

Недоліком порогового методу також є низька швидкість генерування ПВП, оскільки за одну ітерацію можливо отримати тільки один біт послідовності. Збільшити швидкість генерування ПВП можна шляхом бітового представлення хаотичних чисел.

Гістограму будь-якої хаотичної системи при програмній реалізації на ЕОМ формують значущі біти двійкового представлення даних. Відкинувши частину біт, що не відповідають критерію збалансованості, можна отримати послідовності з рівномірним розподілом.

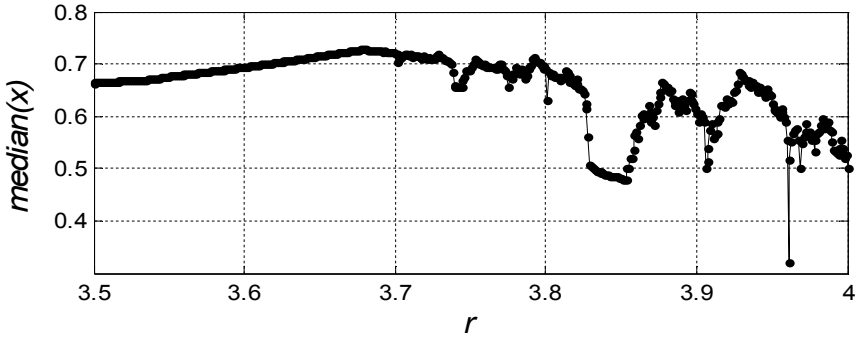


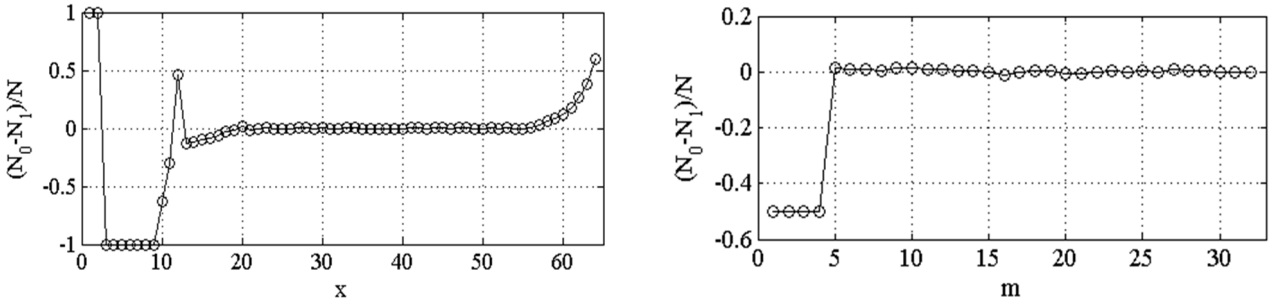
Рис. 4. Залежність медіани розподілу реалізацій системи (1) від параметру керування *r*.

Розглянемо особливості бітового представлення чисел при розрахунках з фіксованою та плаваючою комою і подвійною точністю. Сформуємо матрицю з розмірністю $n \times m$ з елементами $l_{n,m}$.

$$\begin{cases} l_{11} \; . \; l_{12} \; \ldots \; l_{1,\,m} \\ l_{21} \; . \; l_{22} \; \ldots \; l_{2,\,m} \\ \quad . \quad . \quad \ldots \quad . \\ l_{n,1} \; . \; l_{n,2} \; \ldots \; l_{n,\,m} \end{cases} \tag{4}$$

де n – номер ітерації x_n, а m – порядковий номер біта в бінарному представленні дійсного числа.

Для кожного стовпця обчислюється кількість нулів “0” - N_0 та одиниць “1” - N_1, $(N_0 + N_1 = N)$. Залежності відносної різниці кількості «0» і «1» від номера двійкового символу у числі приведено на рис. 5.



а *б*

Рис. 5. Збалансованість послідовностей для логістичного рівняння при *r* = 3.999 для подвійної точності – *а*; арифметики Q3.29 – *б*.

Як випливає із рис. 5 *а*, для подвійної точності найбільш значущі біти, які формують хаотичний атрактор (1) є незбалансованими. Відхилення в пропорції «0» і «1» для найменш значущих бітів обумовлена особливостями округлення в арифметиці з плаваючою комою. Молодші біти збалансовані при реалізації логістичного відображення на ПЛІС та у комп’ютерних обчисленнях з використанням арифметики з фіксованою комою (рис. 5*б*).

Приклад отримання рівномірного розподілу чисел, отриманих на основі реалізацій (1) шляхом відкидання старших 15 біт, приведено на рис. 6 .

4. Ключовий простір. Під простором ключів в методах шифрування на базі детермінованого хаосу розуміють множину значень параметрів та початкових умов, за яких мають місце хаотичні режими. Дуже часто при зміні параметрів хаотичні коливання можуть

переходити в періодичні. Наприклад, для логістичного рівняння хаотичні коливання можуть мати місце при $r \geq 3,57$.

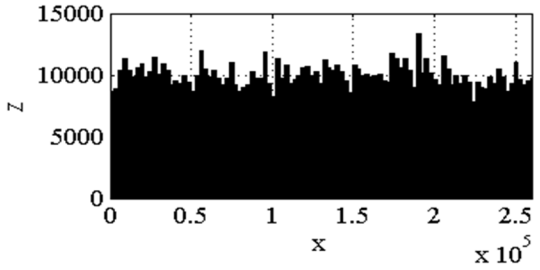


Рис. 6. Гістограма значень часових рядів генерованих (1) при r = 3.999, n=1000000 при відкиданні старших 15 біт при Q3.29.

З діаграми біфуркацій (рис. 7) випливає, що для деяких значень параметру r існують вікна періодичності, внаслідок чого точна оцінка простору ключів унеможливлена.

Тому при виборі хаотичних систем перевагу надавати таким, що характеризуються суцільною діаграмою біфуркацій без вікон періодичності.

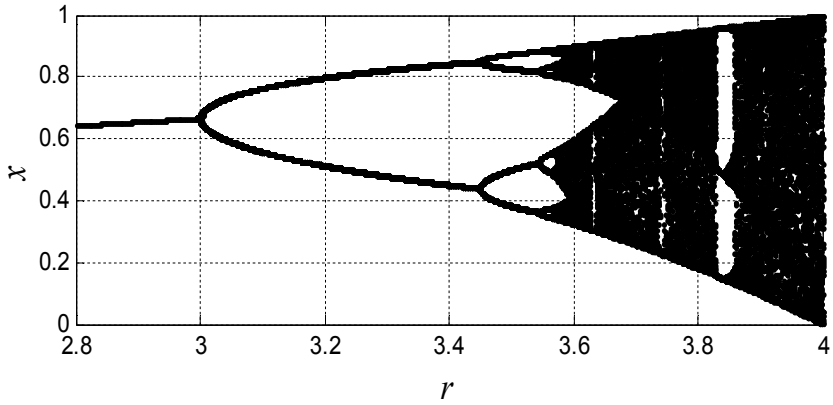


Рис. 7. Біфуркаційна діаграма (1).

Використання всієї множини початкових умов з області притягування атрактора при виборі простору ключів є некоректним і призводить до неправильної оцінки його обсягу. Для системи (1) допустимі значення початкових умов належного діапазону [0, 1], і не залежать від значень параметру r. Розмах хаотичних реалізацій після закінчення перехідного процесу не виходитиме за межі інтервалу (x_{min}, x_{max}) (див. рис 8). При зміні параметру r буде змінюватися розмах реалізацій та обсяг ключового простору початкових умов.

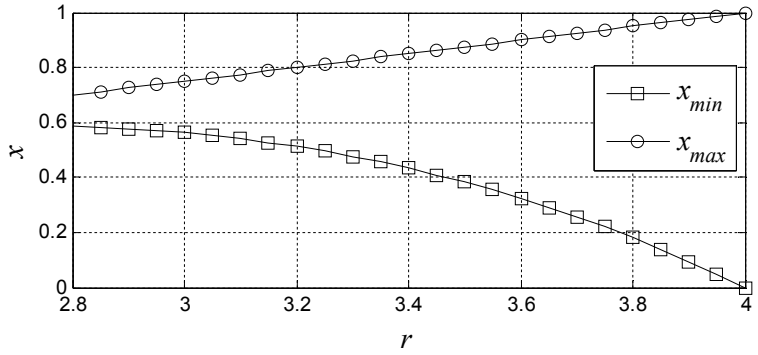


Рис. 8. Обмеження області значень реалізацій логістичного рівняння після перехідного процесу

Легко показати, що послідовність розв'язків (1), що стартують при довільних початкових умовах з області (0,1) з часом обмежиться діапазоном $\left[\frac{r^2}{4}\left(1-\frac{r}{4}\right), \frac{r}{4}\right]$, що і буде ключовим

простором для системи (1). Залежність простору від параметра ускладнює оцінку надійності шифру.

Слід зауважити, що при комп'ютерних обчисленнях різні початкові умови призводять до однакових циклів. Тобто при шифруванні великих обсягів інформації (відносно до середньої тривалості перехідного процесу), початкові умови є слабшим ключем в порівнянні зі значенням параметру керування. Тому при оцінюванні криптостійкості хаотичних шифрів до врахування всієї множини допустимих початкових умов, як простору ключів необхідно підходити з обережністю.

5. Приклади систем з хаотичними режимами неперервними за параметром. Гіперхаотична система Тратаса [5] допускає збільшення розмірності шляхом кільцевого з'єднання підсистем, і у багатовимірному випадку описується наступними рівняннями [18]

$$\begin{cases} x_{n+1}^{(1)} = a_1 \left| x_n^{(1)} \right| - b_1 \left| x_n^{(2)} \right| + 1 \\ x_{n+1}^{(2)} = a_2 \left| x_n^{(2)} \right| - b_2 \left| x_n^{(3)} \right| + 1 \\ \qquad \cdots \\ x_{n+1}^{(p)} = a_6 \left| x_n^{(p)} \right| - b_6 \left| x_n^{(1)} \right| + 1, \end{cases} \tag{5}$$

де a, b – параметри керування, p – розмірність системи, позначення $\left| x_n^{(i)} \right|$ є операцією отримання абсолютного значення $x_n^{(i)}$, $i = [1 \ldots p]$.

Для побудови ПВП запропоновані сімейства систем Лоці, що належать до класу систем з дискретним часом і неперервною множиною значень [19-20]. Одна із таких систем аналітично описується наступними рівняннями [4]:

$$\begin{cases} x_{n+1}^{(1)} = 1 - r \left| x_n^{(1)} \right| + r \left(\left| x_n^{(2)} \right| - \left(x_n^{(1)} \right)^2 \right) \\ x_{n+1}^{(2)} = 1 - r \left| x_n^{(2)} \right| + r \left(\left| x_n^{(3)} \right| - \left(x_n^{(2)} \right)^2 \right) \\ \qquad \cdots \\ x_{n+1}^{(p)} = 1 - r \left| x_n^{(p)} \right| + r \left(\left| x_n^{(1)} \right| - \left(x_n^{(p)} \right)^2 \right) \end{cases}, \tag{6}$$

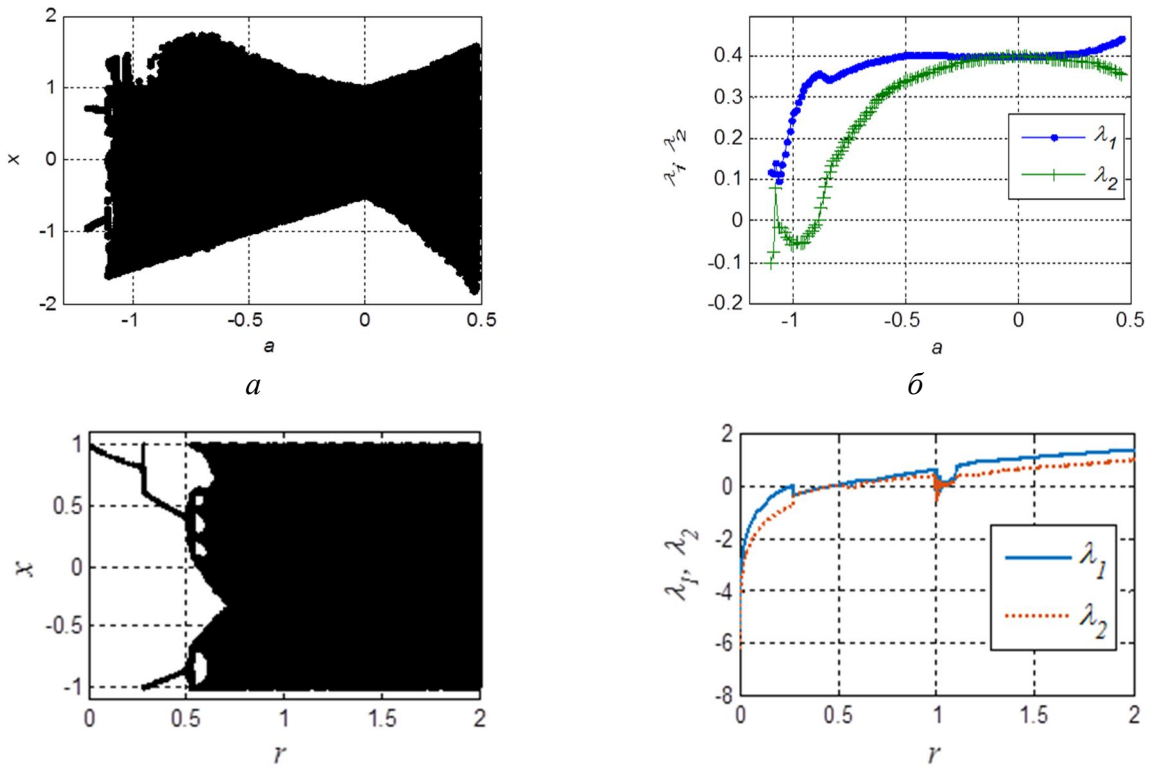
$$\begin{cases} \text{якщо} \quad 1 - r \left| x_n^{(i)} \right| + r \left(\left| x^{(i-1)} \right| - (x_n^{(i)})^2 \right) < -1, \quad x_{n+1}^{(i)} = x_{n+1}^{(i)} + 2, \\ \text{якщо} \quad 1 - r \left| x_n^{(i)} \right| + r \left(\left| x^{(i-1)} \right| - (x_n^{(i)})^2 \right) > 1, \quad x_{n+1}^{(i)} = x_{n+1}^{(i)} - 2, \end{cases} \tag{7}$$

де r – параметр керування, p – розмірність системи, позначення $\left| x_n^{(i)} \right|$ є операцією отримання абсолютного значення $x_n^{(i)}$, $i = [1 \ldots p]$.

Як слідує з біфуркаційних діаграм та значень показників Ляпунова, приведених на рис. 9, для систем (5) і (6), існують області значень параметрів керування, в яких відсутні вікна періодичності. Розмах реалізацій системи Лозі знаходиться в межах [-1, 1] і при значеннях параметру $r \in [1.2,\ 2]$ спостерігається неперервні за зміною параметра гіперхаотичні коливання. Перевагою системи (6) в порівнянні з (5) є майже рівномірний розподіл реалізацій [20].

6. Висновки. В роботі проаналізовано критерії вибору детермінованих хаотичних систем для розробки ГПВП. Досліджено збалансованість послідовностей при використанні арифметики з фіксованою або плаваючою комою. Запропоновано використання багатовимірних відображень з суцільною біфуркаційною діаграмою, що дає змогу уникнути

використання слабких ключів. Показано, що при розробці криптографічних засобів на базі хаотичних систем необхідно враховувати взаємозв'язки між періодичністю, точністю та платформою реалізації.



а *б* *в* *г*

Рис. 9. Характеристики багатовимірних дискретних систем: біфуркаційна діаграма – (*а*), діаграма показників Ляпунова – (*б*) для двовимірної системи Лозі; біфуркаційна діаграма – (*в*), діаграма показників Ляпунова – (*г*) для двовимірної системи Тратаса при $b = 1,493$.

Список використаної літератури

1. Rodriguez-Vazquez A. Chaos from Switched-Capacitor Circuits: Discrete Maps / A. Rodriguez-Vazquez, J. Huertas, A. Rueda, B. Perez-Verdu, and L. O. Chua // Proc. of the IEEE, Special Issue on Chaotic Systems. - Aug. 1987. - PP. 1090-1106

2. Pecora Louis M / Synchronization in chaotic systems / Louis M. Pecora and Thomas L. Carroll // Phys. Rev. Lett. – 1990. - 64, - C. 821.

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

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

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

6. Stojanovski Toni Chaos-Based Random Number Generators—Part I: Analysis / Toni Stojanovski, Ljupco Kocarev // IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS. 2001. - Vol. 48, № 3, - C. 281.

7. IEEE, "IEEE standard Floating-Point Arithmetic," IEEE Std 754-2008, pp. 1-58, Aug., 2008.

8. Чорний А.О. Періодичність розв’язків хаотичних систем при обчисленнях з фіксованою комою / А.О. Чорний, С.Д. Галюк. // Проблеми інформатики та комп’ютерної

техніки: Праці IV-ї Міжнародної науково-практичної конференції, 26 – 29 травня 2015р.: тези доп. – Чернівці, 2015. – С. 157-158.

9. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Телекомунікаційні та інформаційні технології. – 2016. - № 4.

10. Скобелев В.Г. Анализ системы Лоренца над кольцом Z_{p^k} / В.Г. Скобелев // Вестник Томского государственного университета. Приложение. – 2006. – № 17. – С. 134–139.

11. Скобелев В. Г. Комбинаторно-алгебраические модели в криптографии / В.Г. Скобелев // Прикладная дискретная математика. Приложение. 2009. № 2. С. 74–114.

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

13. 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.

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

15. 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.

16. Zhang Xuefeng Extended Logistic Chaotic Sequence and Its Performance Analysis / Zhang Xuefeng, Fan Jiulun // Tsinghua science and technology. – 2007. - Volume 12, Number S1. – PP. 156-161.

17. Галюк С.Д., Генерування псевдовипадкових послідовностей на базі дискретних хаотичних систем / С.Д. Галюк, Л.Ф. Політанський // Міжнародна науково-практична конференція «PREDT-2014 ». – Чернівці: 23-25 жовтня 2014 р. – С. 85-86.

18. Krulikovskyi O.V. PRNG BASED ON MODIFIED TRATASHYPERCHAOTIC SYSTEM FPGA / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Сучасний захист інформації. – 2016. - №2.

19. Garasym Oleg Application of observer-based chaotic synchronization and identiability to original CSK model for secure information transmission / Oleg Garasym, Ina Taralova, Rene Lozi. // Indian Journal of Industrial and Applied Mathematics. – 2015. - № 6 (1). - PP.1-26.

20. Oleg Garasym Exploring some topologies of coupled chaotic networks / Oleg Garasym, Ina Taralova, Rene Lozi. // International Workshop on Nonlinear Maps and their Applications «NOMA-2015». - Dublin, Ireland: Jun 2015. - PP. 34-39.

References

1. Rodriguez-Vazquez A. Chaos from Switched-Capacitor Circuits: Discrete Maps / A. Rodriguez-Vazquez, J. Huertas, A. Rueda, B. Perez-Verdu, and L. O. Chua. // Proc. of the IEEE, Special Issue on Chaotic Systems. - Aug. 1987. - PP. 1090-1106

2. Pecora Louis M / Synchronization in chaotic systems / Louis M. Pecora and Thomas L. Carroll // Phys. Rev. Lett. – 1990. - 64, - C. 821.

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

4. Pticzy'n N. Application of the theory of deterministic chaos in cryptography / N. Pticzy'n. – Moscow: MGTU N.E'. Baumana, 2002. – 80 p.

5. Shahtarin B.I. Generators of chaotic oscillations / B.I. Shahtarin, P.I. Koby'lkina, Yu.A. Sidorkina, A.V. Kondrat"e'v, S.V. Mitin. Moscow: Galileos ARV. –2007. – 247 p.

6. Stojanovski Toni Chaos-Based Random Number Generators—Part I: Analysis / Toni Stojanovski, Ljupco Kocarev // IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS. 2001. - VOL. 48, № 3, - C. 281.

7. IEEE, "IEEE standard Floating-Point Arithmetic," IEEE Std 754-2008, pp. 1-58, Aug., 2008.

8. Chornyi A.O. Periodicity of chaotic systems solutions at calculations with fixed point / Chornyi A.O. , S.D. Haliuk. // Informatics and Computer Technics Problems: Proceedings of the IV-th International scientific and practical conference, 26 – 29 may 2015: Chernivtsi, 2015. – PP. 157-158.

9. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Telekomunikatsiini ta informatsiini tehnolohii. – 2016. - № 4.

10. Skobelev V.G. Analysis of the Lorentz system over the ring Z_{p^k} / V.G. Skobelev // Bulletin of Tomsk State University. Application. – 2006. – № 17. – PP. 134–139.

11. Skobelev V.G. Combinatorial-algebraic models in cryptography / V.G. Skobelev // Applied Discrete Mathematics. Supplement. - 2009. - № 2. pp. 74–114.

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

13. 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.

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

15. 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.

16. Zhang Xuefeng Extended Logistic Chaotic Sequence and Its Performance Analysis / Zhang Xuefeng, Fan Jiulun // Tsinghua science and technology. – 2007. - Volume 12, Number S1. – PP. 156-161.

17. Haliuk S.D. Generation of pseudorandom sequences based on discrete chaotic systems / S.D. Haliuk, L.F. Politanskyi // Proceedings of the International scientific and practical conference «PREDT-2014 ». – Chernivtsi: 23-25 october 2014. – PP. 85-86.

18. O. V. Krulikovskyi PRNG based on modified tratashyperchaotic system FPGA / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Suchasnyi zahyst informatsii. – 2016. - №2.

19. Oleg Garasym Application of observer-based chaotic synchronization and identiability to original CSK model for secure information transmission / Oleg Garasym, Ina Taralova, Rene Lozi. // Indian Journal of Industrial and Applied Mathematics. – 2015. - № 6 (1). - PP.1-26.

20. Oleg Garasym Exploring some topologies of coupled chaotic networks / Oleg Garasym, Ina Taralova, Rene Lozi. // International Workshop on Nonlinear Maps and their Applications «NOMA-2015». - Dublin, Ireland: Jun 2015. - PP. 34-39.

Автори статті

Круліковський Олег Валерійович – аспірант кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича.. E-mail: o.krulikovskyi@chnu.edu.ua

Галюк Сергій Дмитрович – к.т.н, асистент кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Тел.: +380 (66) 148 7945. E-mail: s.haliuk@chnu.edu.ua

Політанський Леонід Францович – д.т.н., професор, завідувач кафедри радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича. E-mail: l.politansky@chnu.edu.ua

Authors of the article

Krulikovskyi Oleh Valeriiovych – PhD student of radio engineering and information security department, Yuriy Fedkovych Chernivtsi National University, E-mail: o.krulikovskyi@chnu.edu.ua

Haliuk Serhii Dmytrovych– PhD, assistant professor of radio engineering and information security department, Yuriy Fedkovych Chernivtsi National University,. Tel.: +380 (66) 148 7945. E-mail: s.haliuk@chnu.edu.ua

Politanskyi Leonid Frantsovych – doctor of sciences (technical), professor, head of radio engineering and information security department, Yuriy Fedkovych Chernivtsi National University, E-mail: l.politansky@chnu.edu.ua

Дата надходження
в редакцію: 17.03.2017 р.

Рецензент:
доктор технічних наук, професор В. П. Тарасенко
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»