УДК 621.372

П.В. Іванюк, Р.Л. Політанський, Л.Ф. Політанський
Національний університет "Львівська політехніка"

ХАРАКТЕР РОЗПОДІЛУ ПАРАМЕТРІВ ПСЕВДОВИПАДКОВОЇ ПОСЛІДОВНОСТІ, ЗГЕНЕРОВАНОЇ КАРТОЮ БЕЙКЕРА

Псевдовипадкові числа відіграють важливу роль при побудові дуже багатьох алгоритмів захисту мережі. До таких алгоритмів належать: схеми взаємної ідентифікації, генерування сеансових ключів, генерування ключів алгоритму RSA шифрування з відкритим ключем тощо [1].

Алгоритми генерування псевдовипадкових послідовностей бітів називають картами хаосу.

У цій роботі було досліджено властивості карти хаосу, яку називають картою Бейкера [2]:

$$X_{n+1} = \begin{cases} 2X_n, коли 0 \le X_n < \frac{1}{2} \\ 2(1 - X_n), коли \frac{1}{2} \le X_n < 1 \end{cases} \quad (1)$$

Її аналітичний розв'язок має такий вигляд:

$$X_n = \frac{1}{p}\arccos\left(\cos 2^n \cdot p \cdot x_0\right) \quad (2)$$

Розширимо загальну формулу до вигляду:

$$X_n = \frac{1}{p}\arccos\left(\cos k^n \cdot p \cdot x_0\right), \text{ для } k>2. \quad (3)$$

Досліджувані послідовності, генеровані нелінійними функціями, мають властивості, відмінні від властивостей послідовностей, що генеровані лінійними системами.

Послідовності, генеровані лінійними системами, характеризуються певними вимогами.

Збалансованість – різниця між кількістю бітів, що мають значення "0" і "1".

Циклічність – визначення кількості циклів з різними довжинами бітів. Під циклом розуміють неперервну послідовність однакових двійкових чисел. Виникнення іншої двійкової цифри автоматично розпочинає новий цикл. Довжина циклу дорівнює кількості цифр у такому циклі.

Кореляція – показник, що дорівнює різниці кількості збігів і незбігів у значеннях бітів, виміряних для послідовності, зсунутої на 1 біт відносно початкової, розділеній на довжину послідовності.

Для генерування послідовності і дослідження її властивостей створено відповідні програми у середовищі Microsoft Visual C++ 6.0.

Кожний наступний біт послідовності $B(x_0) = \{b_1, b_2, ..., b_n\}$ утворюється за правилом:

$$b_n = \begin{cases} 0, \text{ при } x_n \in \mathrm{X}_0 \\ 1, \text{ при } x_n \in \mathrm{X}_1 \end{cases} \quad (4)$$

Множини X_0 і X_1 є неперервними відрізками дійсних чисел однакової довжини: $(0;1/2]$ та $[1/2;1)$ відповідно.

Значення породжувального числа x_0 змінювалися на проміжку $(0;1)$ з кроком, що дорівнює $0{,}1$.

На рис. 1 наведена схема генерування бітів псевдовипадкової послідовності.

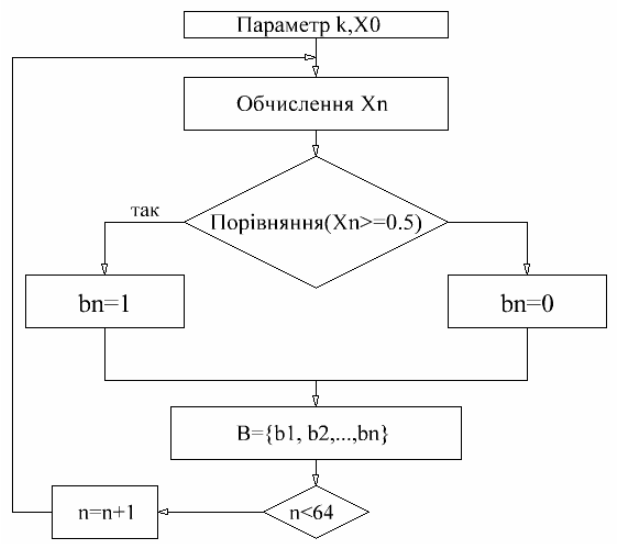


Рис. 1. Блок-схема генерування бітів псевдовипадкової послідовності

Досліджувались послідовності довжинами 64, 128, 256, 512, 1024. Оскільки обмеження за модулем для типу double в C++ дорівнює 10^{308}, то існує верхня межа для n, яку знаходимо зі співвідношення $k^n = 10^{308}$ (табл. 1).

Таблиця 1

Гранична довжина послідовності залежно від параметра k

k	Довжина послідовності, n
64938	64
254	128
16	256
4	512
2	1024

Як видно із рис. 2, розподіл густини ймовірностей збалансованості послідовностей, усереднений за значеннями параметра x_0, є близьким до розподілу Гаусса із середнім значенням $M(L) = 0$ та дисперсією $s_0^2 = 6.47$.

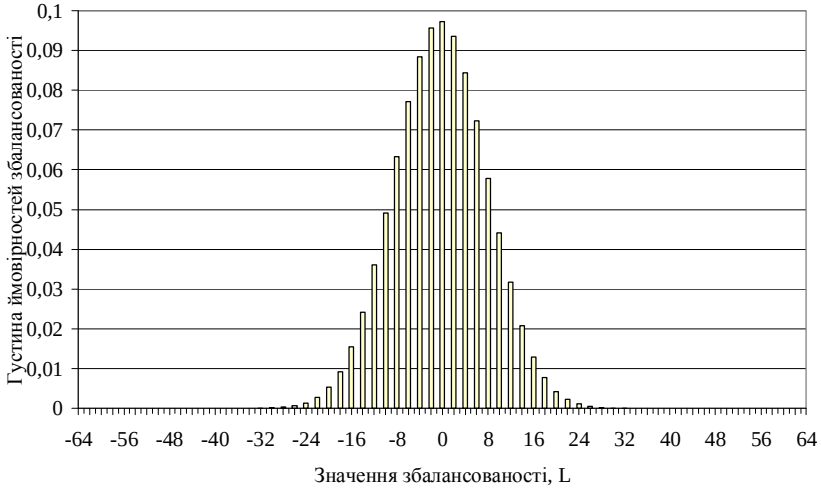


Рис. 2. Розподіл густини ймовірностей збалансованості послідовностей, усереднений за значеннями параметра x_0

Дослідження циклічності послідовностей довжиною 64 біти здійснювали для циклів з довжинами 1, 2, 3 біти, 4-11 бітів та більше ніж 11 бітів. У табл. 2 наводяться і порівнюються значення внесків бітів генерованої послідовності та лінійної системи для породжувального числа $x_0 = 0.4$.

Таблиця 2

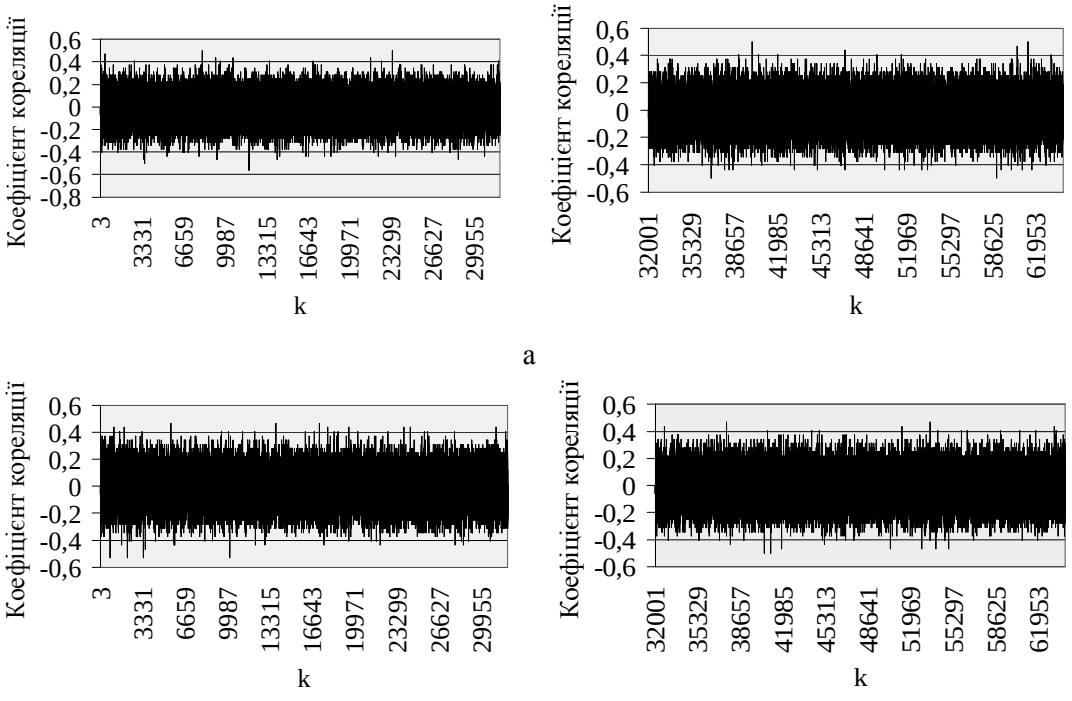
Циклічність лінійних систем і систем на основі карти хаосу

Лінійні системи					
Довжина послідовності	64				
Довжина циклів, бітів	1	2	3	4-11	>11
Відносна кількість бітів, %	50	25	12,5	12,45117	0,04883
Кількість циклів	32	8	3	2	0
Абсолютна кількість бітів	32	16	8	7,97	0,03
Системи на основі карти хаосу					
Довжина послідовності	64				
Середнє значення і середньоквадратичне відхилення кількості циклів	16,79±4,49	7,31±2,51	3,86±1,77	3,81±1,48	0,01±0,11
Середнє значення і середньоквадратичне відхилення абсолютної кількості бітів	16,79±4,49	14,63±5,04	11,59±5,31	18,81±7,46	0,17±1,50
Середнє значення і середньоквадратичне відхилення відносної кількості бітів, нормованої на довжину послідовності, %	26,23±7,02	22,86±7,88	18,11±8,30	28,39±11,66	0,27±2,34

Визначення коефіцієнта кореляції здійснювалось порівнянням кожного біта отриманої послідовності з відповідним бітом наступної послідовності, зсунутої на 1 біт ліворуч з подальшим обчисленням різниці між кількістю збігів та кількістю незбігів, нормованим на довжину періоду [3]:

$$K = \frac{Число_{збігів} - Число_{розбіжностей}}{Довжина\_періоду} \qquad (5)$$

Залежність кореляції від параметра k наведена на рис. 3.



а

б

Рис. 3. Залежність коефіцієнта кореляції від зміщення:
а – значення породжувального елемента x_0 =0,3; б – x_0 =0,6

На рис. 4 наведено розподіл коефіцієнтів кореляції на множині значень параметра k. Послідовність не є періодичною (для періодичних послідовностей модуль коефіцієнта автокореляції близький до 1). Середнє (в статистичному сенсі) значення автокореляції дорівнює 0. Коефіцієнт автокореляції лежить у межах від –0,4 до 0,4.

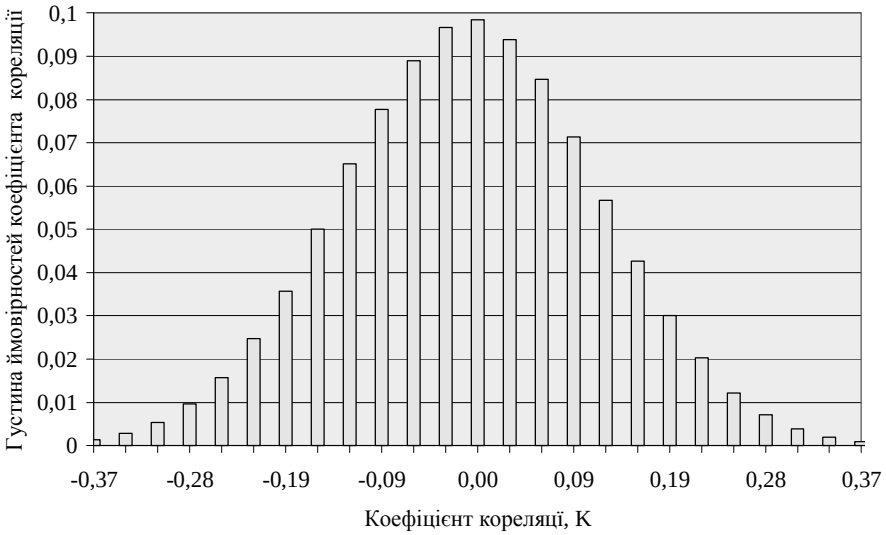


Рис. 4. Розподіл густини ймовірності кореляції на множині значень параметра k

Висновки:

1. Розподіл густини ймовірностей збалансованості є близьким до розподілу Гаусса із середнім значенням $M(L)=0$ та дисперсією $s_0^2 = 6.47$.

2. Показники циклічності, генеровані досліджуваною картою, відрізняються від показників генерованих лінійними системами. Вони гірші внаслідок досить великого внеску циклів великої довжини (4–11).

1. Вильям Столингс. Криптография и защита сетей. – 2-е изд. – М.: Издательский дом "Вильямс", – 2001, 670 с. 2. Y. Mao et al.: A Chip Performing Chaotic Stream Encryption. Studies in Computional Intelligence (SCI) 42, 307-332 (2007). 3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – Изд. 2-е, испр.; Пер. с англ. – М.: Издательский дом "Вильямс", 2007. – 1104 с.