УДК 621.39
© З. Готра[1], Р. Політанський[1], 2010

ВЛАСТИВОСТІ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ГЕНЕРОВАНИХ КАРТАМИ ХАОСУ

Досліджено псевдовипадкові послідовності, що генеруються картами хаосу. Описано їх властивості та особливості, відповідно до отриманих результатів.

The pseudorandom sequences, generated by chaos maps were investigated in this paper. These features were described according to the obtained results.

Розвиток засобів комунікації призвів до виникнення схем передавання даних, що використовують генератори сигналів з властивостями хаотичних систем. Такі генератори можуть бути одно- та багатовимірними. В літературних джерелах виникла спрощена назва таких схем – генератори хаосу.

Застосування генераторів хаосу у схемах передавання даних має декілька аспектів: додавання хаотичного сигналу до сигналу даних, використання хаотичного сигналу в якості ключа у потоковому шифруванні, можлива також комбінація таких застосувань: в таких схемах неможливо відділити передавання даних від шифрування сигналів. В таких схемах здійснюється кодування інформації з нелінійним підмішуванням інформаційного сигналу. Схема такого процесу представлена на рис.1.

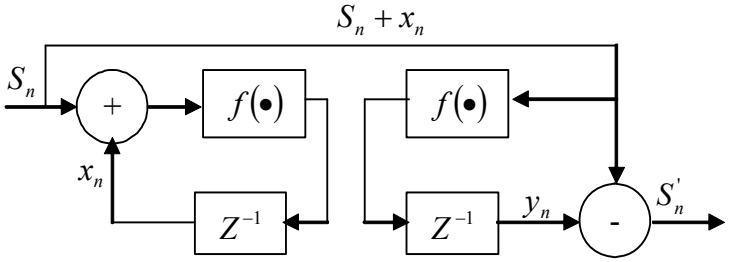


Рис. 1. Схема кодування з нелінійним підмішуванням інформаційного сигналу. S_n – інформаційний сигнал, x_n – хаотичний сигнал

[1] Національний університет «Львівська політехніка»

Однією з задач, що виникають при роботі із схемами на базі генераторів хаосу, є генерування хаотичних сигналів, що отримали назву псевдо випадкових послідовностей [1].

В роботі приводяться результати дослідження властивостей псевдовипадкових послідовностей, генерованих картою хаосу, що має аналітичний розв'язок наступного вигляду [2]:

$$x_n = \sin^2\left(2^n * \arcsin\left(\sqrt{x_0}\right)\right) \quad (1)$$

Генерування бітів псевдовипадкової послідовності $B(x_0) = \{b_1, b_2, ..., b_n\}$, утвореною картою хаосу, відбувається з використанням наступного алгоритму:

$$b_n = \begin{cases} 0, \text{при } x_n \in \mathrm{X}_0 \\ 1, \text{при } x_n \in \mathrm{X}_1 \end{cases} \quad (2)$$

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

Значення породжувального числа (числа x_0) елемента змінювалися на проміжку $(0;1)$ з кроком рівним $0{,}01$.

Використання базових типів змінних неминуче призводить до обмежень довжини послідовностей, отримуваних програмними засобами. Обчислення, що проводяться з великими за модулем числами є специфічними для задачі генерування псевдовипадкових послідовностей. При значеннях n порядка 1000 і більше виникає необхідність здійснювати обчислення з числами, які перевищують за модулем максимально можливе значення для змінних базового типу C++ double ($1{,}8 * 10^{308}$). Тому довжина послідовностей бітів не може перевищувати 1024. При $n > 1024$ значення всіх бітів дорівнює 0.

Дослідження властивостей збалансованості, циклічності, кореляції (періодичності) псевдо випадкових послідовностей здійснювалися за критеріями, приведеними в [1]. В роботі [1] описаний зміст і спосіб знаходження вказаних величин для псевдовипадкових послідовностей, генерованих схемами, що містять елементи LFSR (Linear Feedback Shift Register) – лінійні зсувові регістри із зворотнім зв'язком. Логічна схема зображена на рис. 2.

Робота регістра відбувається таким чином: при надходженні синхросигналу значення із запам'ятовувального елемента регістра записується в наступний за напрямком стрілки. Значення першого елемента є елементом генерованої послідовності. В останню комірку записується сума значень елементів, які вносять вклад у зворотній зв'язок.

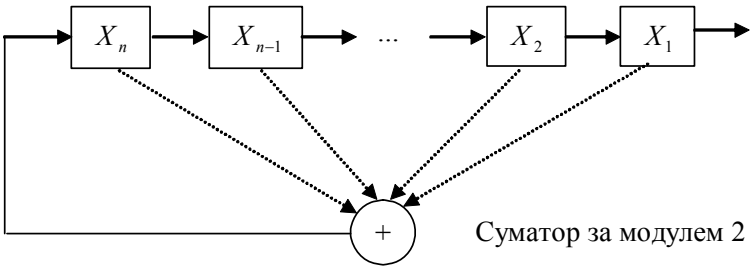


Рис. 2. Схема n – каскадного регістра із зворотним зв'язком

Така послідовність є періодичною із значенням періоду $2^n - 1$. Генерована послідовність залежить від елементів, що вносять вклад у зворотній зв'язок (структура схеми) і від початкового стану регістра (ключ схеми).

Опишемо зміст вказаних властивостей і методику за якою були отримані числові значення.

Збалансованість – це різниця між кількістю бітів, що мають значення «0» і кількістю бітів, що мають значення «1», що вимірюється на періоді послідовності. Для лінійних схем приводиться значення, що дорівнює 1.

Циклічність – виражає кількісний вклад у псевдовипадкову послідовність бітів із однаковими значеннями, які слідують один за одним. Набір бітів, що мають однакове значення і слідують один за одним у загальній послідовності називають циклами, тобто якщо значення наступного біта відрізняється від попереднього, розпочинається новий цикл. Для лінійних схем приведені такі критерії: : кількість бітів у циклах довжиною 1 становить 50% від довжини, у циклах довжиною 2 – 25%; у циклах довжиною 3 –12,5% і т.д. Таким чином, сумарний вклад циклів довжиною 4 і більше становить 12,5%.

Значення автокореляції складає $-1/p$, де p – це довжина періоду послідовності. Вказані характеристики обчислюють для послідовності, довжина якої дорівнює періоду послідовності бітів.

Дослідження властивостей корельованості для нелінійних схем вимагають додаткового розгляду питання, чи є такі послідовності періодичними. Складність дослідження таких систем полягає в тому, що вони не є періодичними у класичному розумінні.

А метод, описаний в [1], є прийнятним для послідовностей, генерованих схемами на базі LFSR, які є періодичними.

Дослідження властивості періодичності для вказаної послідовності здійснювалася шляхом обчислення кореляції між послідовностями

певної довжини, які слідують одна за одною. Тобто досліджувалися послідовності усіх можливих довжин (від 1 до 512), які є фрагментами загальної послідовності. Для фіксованої довжини обчислювали коефіцієнт кореляції між послідовностями, зміщеним на вказану довжину (у припущенні, що така довжина є періодом). Далі коефіцієнт кореляції усереднювався: обчислювалися коефіцієнти кореляції між усіма можливими послідовностями вибраної довжини. Таким чином отримали залежність коефіцієнта кореляції від довжини послідовності, у припущенні, що така довжина є періодом.

Коефіцієнт автокореляції обчислюємо за формулою:

$$k = \frac{Число_{співпадань} - Число_{розбіжностей}}{Довжина\_періоду}$$

На рис. 3 приведені 4 характерні графіки (для різних значень породжувального числа), що відображають залежність коефіцієнта кореляції від довжини послідовності у припущенні, що вибрана довжина є періодом.

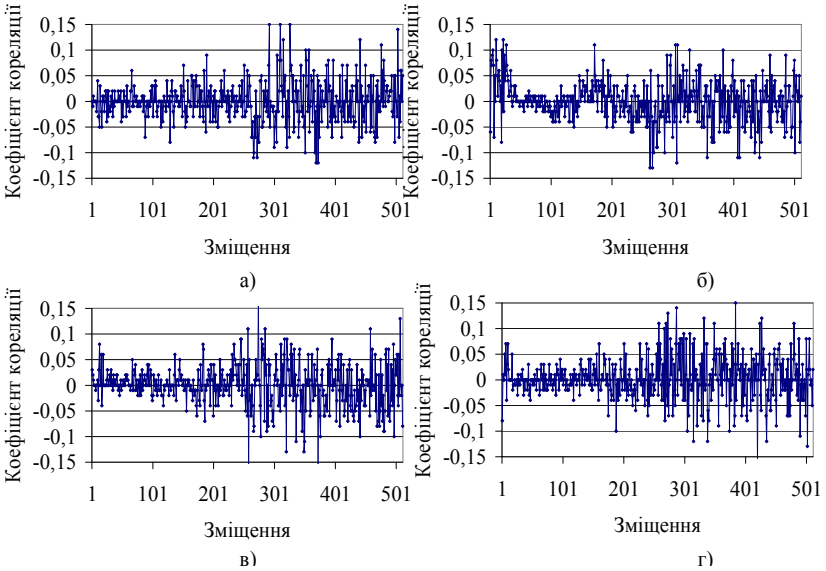


Рис. 3. Залежність кефіцієнта кореляції від зміщення. а) значення породжувального елемента а) x_0=0,05; б) x_0=0,25; в) x_0=0,56; г) x_0=0,87;

Якщо б коефіцієнт кореляції виявився близьким до 1, можна було б сказати, що послідовність має період в статистичному розумінні.

Вимірювання проводились для можливих значень породжувального числа x_0 (від 0 до 1 з кроком 0,01).

Але для всіх можливих довжин (від 1 до 512) модуль кореляції виявився суттєво меншим за одиницю і в межах від $-0{,}15$ до $+0{,}15$.

Псевдовипадкова послідовність, отримана авторами роботи не є періодичною, тому для здійснення обчислень були вибрані фрагменти послідовності максимальної довжини 1024 біт, що є характерними для криптографії: 64, 128, 256, 512.

У межах точності чисельного моделювання було зроблено висновок про те, що карти хаосу є чутливими до значень породжувального параметру, про що говорить якісний аналіз послідовності (рис.4, рис.5).

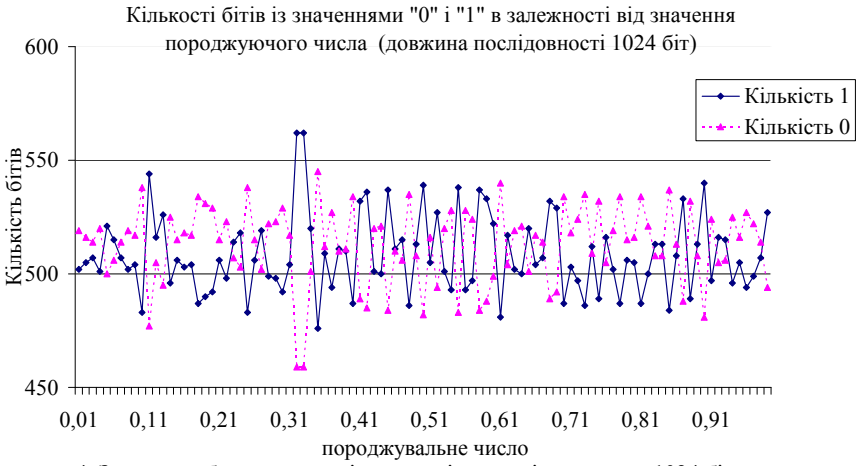


Рис. 4. Значення збалансованості для послідовності довжиною 1024 біти (приведені кількості бітів, що мають значення «1» і «0»)

Залежність збалансованості від довжини послідовності приведена на рис.6.

В таблицях 1, 2 відображені агреговані дані чисельного експерименту по збалансованості і циклічності.

Значення циклічності значно відрізняються від значень, отриманих на елементах LSFR (рис.7). Виявилося, що циклічність не залежить від довжини досліджуваного фрагмента і становить 25% для циклів довжиною 1 і довжиною 2 біти, 20 відсотків для циклів довжиною 3 біти і 30 відсотків для циклів довжиною 4 біти і більше. Із зменшенням довжини послідовності значно зростає статистична недостовірність, тому довжина 64 найменша із досліджуваних.

Статистична недостовірність для циклічності значно менша ніж для збалансованості: у найгіршому випадку значення середньоквадратичного відхилення складає 30% від середнього значення (для збалансованості – 80%).

Таблиця 1

Середнє значення розбалансованості (абсолютне значення різниці між кількістю бітів із значенням «1» і кількістю бітів із значенням «0», в дужках вказане значення приведене до довжини послідовності)

Довжина послідовності	Значення розбалансованості
1024	27 (0,027)
512	20 (0,039)
256	15 (0,057)
128	10 (0,076)
64	6 (0,098)

Таблиця 2

Відносна кількість бітів, що містяться у циклах різних довжин на фрагменті довжиною 1024 біти

Довжина циклів	Відносна кількість бітів, %	Відносна кількість бітів для лінійних систем, %
1	24	50
2	25	25
3	19	12,5
4-11	30	12,5

Кореляція досліджувалась на довжинах, які є характерними для криптографії – 512 і 1024 біти. Проведені дослідження показують, що корельованість є досить слабкою (коефіцієнт кореляції знаходиться в межах від $-0{,}01$ до $+0{,}01$). Для вимірювання використовувалась методика викладена вище (послідовність зміщувалася на 1 біт і визначався коефіцієнт кореляції між початковою і зміщеною послідовностями).

Аналогічна характеристика для лінійних послідовностей дорівнює $-1/p$, як показано автором роботи [1]. Тобто для послідовностей, генерованих за допомогою схеми, що містить LSFR, значення кореляції становить $-0{,}002$ і $0{,}0001$.

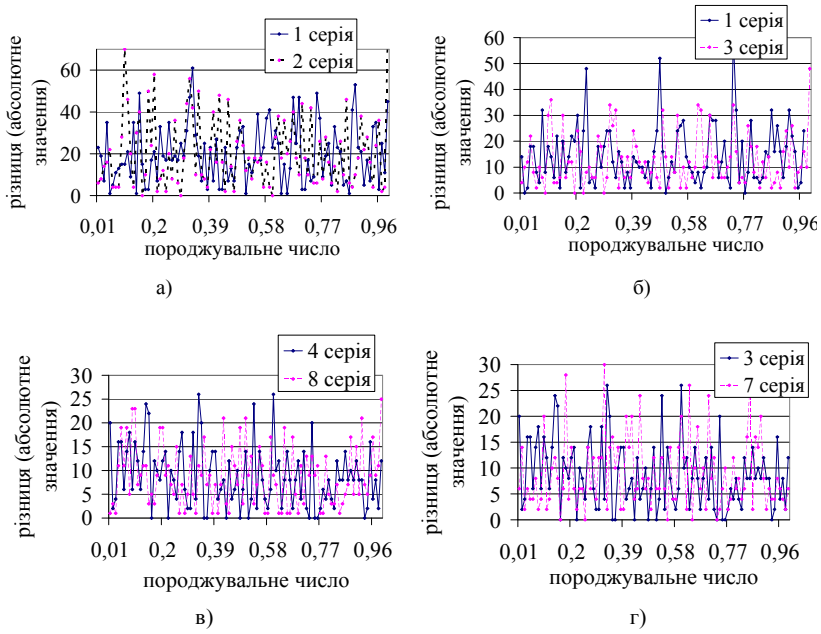


Рис. 5. Значення збалансованості для послідовностей, що мають довжини кратні 64 (приведена різниця між кількостями бітів, що мають значення «0» і «1»). Приведені дані для різних серій, розміщення в середині фрагмента довжиною 1024 біти: а) довжина фрагментів 512 біт; б) 256 біт; в) і г) 128 біт

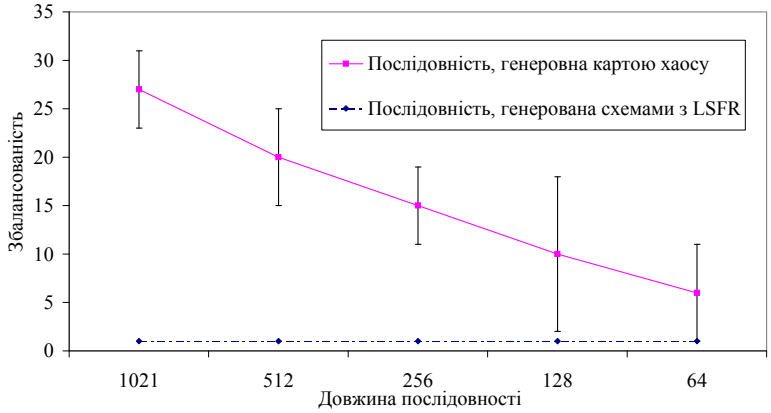
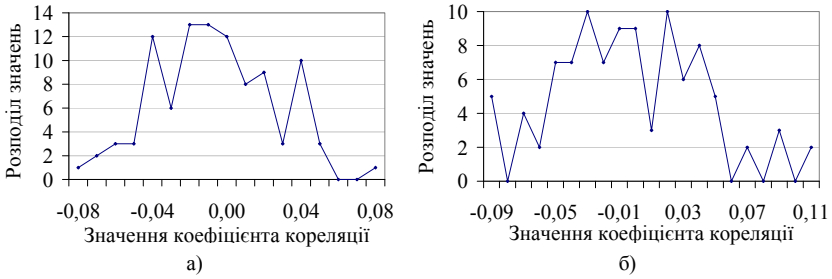


Рис. 6. Залежність збалансованості від довжини послідовності

Очевидно, що для застосувань криптографії корельованість повинна бути якомога меншою. Отже, властивості корельованості для послідовності, генерованої картою хаосу є дещо гіршими у порівнянні з послідовностями, генерованими елементами LSFR.

На рис.7 приведений розподіл значень коефіцієнта кореляції на множині породжувальних чисел.



а) б)

Рис. 7. Розподіл значення кореляції на множині породжувальних елементів: а) послідовність довжиною 1024 біт; б) послідовність довжиною 512 біт

До висновків даної роботи можна віднести такі:

Критерієм періодичності для послідовностей бітів був вибраний коефіцієнт кореляції між фрагментами, зміщеними на таку довжину, яка вважається періодом послідовності.

Послідовність, генерована картою хаосу не виявляє властивостей періодичності з досить високою точністю обчислень. На досліджуваних довжинах (від 1 до 512) коефіцієнт кореляції виявився в межах від $-0{,}15$ до $+0{,}15$.

Збалансованість залежить від довжини послідовності.

Циклічність не залежить від довжини послідовності.

Коефіцієнт кореляції для фрагментів довжиною 512 і 1024 виявився в межах від $-0{,}01$ до $+0{,}01$.

Показники збалансованості, циклічності і корельованості для послідовностей, генерованих картами хаосу виявилися гіршими за показники послідовностей, генерованих схемами на елементах LSFR.

1. Скляр Бернард. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – М.: Издательский дом «Вильямс», 2007. – 1104 С. 2. Y. Mao et al.: A Chip Performing Chaotic Stream Encryption. Studies in Computional Intelligence (SCI) 42, 307-332 (2007).