УДК 681.5.032

В. Максимович[1], М. Шевчук[1], М. Мандрона[2]
Національний університет "Львівська політехніка",
[1]кафедра безпеки інформаційних технологій,
Львівський державний університет безпеки життєдіяльності,
[2]кафедра управління інформаційною безпекою,

ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ LFSR

Здійснено дослідження генераторів псевдовипадкових бітових послідовностей, побудованих на основі LFSR. Розроблено імітаційні моделі генераторів із різними значеннями твірних поліномів. Досліджено статистичні характеристики генераторів, їх періоди повторення, складність побудови (технологічність) під час реалізації на програмованих логічних інтегральних схемах і максимально можливу довжину криптографічного ключа.

Ключові слова: псевдовипадкова бітова послідовність, генератори псевдовипадкових чисел, статистичні характеристики.

The researching of pseudorandom bit sequences generators that based on LFSR is carried out in the article. The imitation models of generators with different formative polynomials are worked out. The researching of generators statistic characteristics, their repetition period, complication of construction (technologicalness) for realization on programmable logic devices and maximally possible length of cryptographic key was also undertaken.

Key words: pseudorandom bit sequence, pseudorandom number generators, statistic characteristics.

Вступ

Сучасна наука широко використовує генератори псевдовипадкових бітових послідовностей (ГПВБП) у різних системах. У сфері захисту інформації псевдовипадкові числа використовують як у технічних, так і у криптографічних засобах захисту інформації. Відомо, що характеристики систем безпеки залежать від характеристик їх підсистем, які визначаються не тільки використаними алгоритмами, але й якісними показниками використаних псевдовипадкових послідовностей. Оскільки безпека криптосистеми зосереджена на ключі, то під час використання ненадійного процесу генерації ключів уся криптосистема стає вразливою. Тому актуальним є питания побудови якісних, надійних ГПВБП.

Мета роботи – дослідити характеристики ГПВБП, побудованих на основі LFSR, зокрема їх статистичні характеристики і періоди повторення.

Генератори псевдовипадкових бітових послідовностей на основі LFSR

Відомо, що окремо взяті генератори псевдовипадкових бітових послідовностей (ГПВБП) на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (linear feedback shift register) не належать до криптостійких [1, 2]. Незважаючи на це, вони часто використовуються під час реалізації потокових шифрів (наприклад, алгоритми – A3, A5, A8, PIKE, SEAL, RC4) або як структурні елементи складніших пристроїв. Основною їх перевагою є велика швидкодія і простота за апаратної реалізації.

Статистичні характеристики ГПВБП на основі LFSR розглядались у багатьох роботах, зокрема у [1, 2]. Однак залишаються не повністю розв'язаними такі задачі:

- визначення мінімальної кількості структурних елементів LFSR і пристроїв на їх основі, за яких досягається статистична безпека, тобто статистичні характеристики вихідної бітової послідовності є задовільними;
- комплексне порівняння основних характеристик генераторів на основі LFSR з характеристиками генераторів, побудованих на інших базах, наприклад, на основі модифікованих адитивних генераторів Фібоначчі (МАГФ) [3] чи на основі R-блоків [4, 5].

Проведені у цій роботі дослідження скеровані на часткове розв'язання вказаних задач. При цьому вважаємо, що статистичні характеристики ГПВБП є задовільними, якщо вихідна бітова послідовність генератора проходить усі тести NIST [6], а під час комплексного порівняння генераторів на різних базах, окрім їх статистичних характеристик, будемо також розглядати: періоди повторення вихідної послідовності, складність побудови (технологічність) під час реалізації на програмованих логічних схемах (ПЛІС) і максимально можливу довжину криптографічного ключа.

Варто підкреслити, що криптостійкість таких генераторів без криптоаналізу, не є гарантованою. Статистична безпека, як відомо, є для цього необхідною, але не достатньою умовою [7].

Варіанти побудови ГПВБП на основі LFSR необхідно розглядати, враховуючи рівняння його функціонування:

$$Q(t+1) = T^r Q(t), \tag{1}$$

де $Q(t)$ і $Q(t+1)$ – стани регістра у моменти часу t і t+1 (до і після синхроімпульсу); T – квадратна матриця порядку n вигляду:

$$T_1 = \begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ & & & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix} \quad \text{або} \quad T_2 = \begin{vmatrix} 0 & \dots & 0 & 0 & a_n \\ 1 & \dots & 0 & 0 & a_{n-1} \\ & & & & \\ 0 & \dots & 1 & 0 & a_2 \\ 0 & \dots & 0 & 1 & a_1 \end{vmatrix}; \tag{2}$$

n – степінь многочленна:

$$F(x) = \sum_{i=0}^{n} a_i x^i, \quad a_n = a_0 = 1, \quad a_j \in \{0,1\}, \quad j = \overline{1,(n-1)}; \tag{3}$$

r – степінь матриці [1].

Отже, LFSR відрізняються:

- степенем і видом твірного полінома (3), що задають кількість розрядів регістра зеуву і впливають на форму зворотних зв'язків;
- виглядом (T1 чи T2) і степенем r матриці, що задають спосіб формування зворотних зв'язків і формують їх остаточну конфігурацію.

Максимально можливий період повторення станів тригерів LFSR, а отже, і вихідної бітової послідовності дорівнює $2^n - 1$. Умови, за яких період повторення досягає цього значення, залежать від форми многочлена $F(x)$. Многочлен $F(x)$ степеня n називається примітивним, якщо він не ділить націло жоден многочлен вигляду $x^S - 1$, де $S < 2^n - 1$. Послідовність, що формується LFSR, має максимальний період тоді і тільки тоді, коли числа S і r є взаємно простими. За $r = 1$ примітивність $F(x)$ є необхідною і достатньою умовою отримання максимального неріоду повторення [1].

Далі наведемо кілька прикладів генераторів з метою з'ясування мінімальної кількості їх структурних елементів, необхідних для забезпечення статистичної безпеки.

На рис. 1 показана спрощена (без кіл установлення початкового стану) структурна схема ГПВБП на основі LFSR, що відповідає твірному примітивному поліному:

$$F(x) = x^9 + x^4 + 1, \tag{4}$$

до складу якої входять тригери $T_1 - T_9$ і суматор за модулем 2.

У цьому випадку вибраний тип матриці T_1 і степінь матриці $r = 1$.

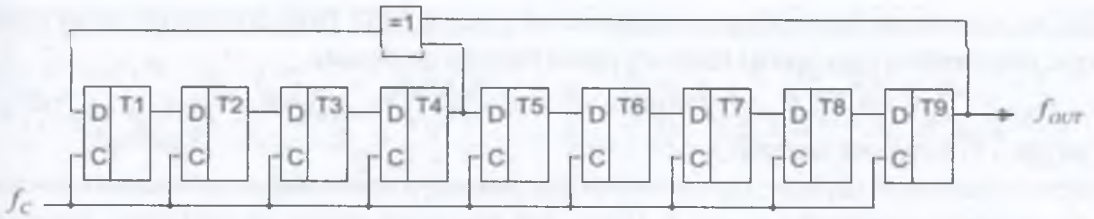


Рис. 1. Спрощена структурна схема ГПВБП на основі LFSR ($F(x) = x^9 + x^4 + 1$)

На рис. 2 показано графік залежності періоду повторения генератора T_P (period) від значення двійкового початкового коду A_0 у регістрі LFSR, отриманий в результаті імітаційного моделювання.

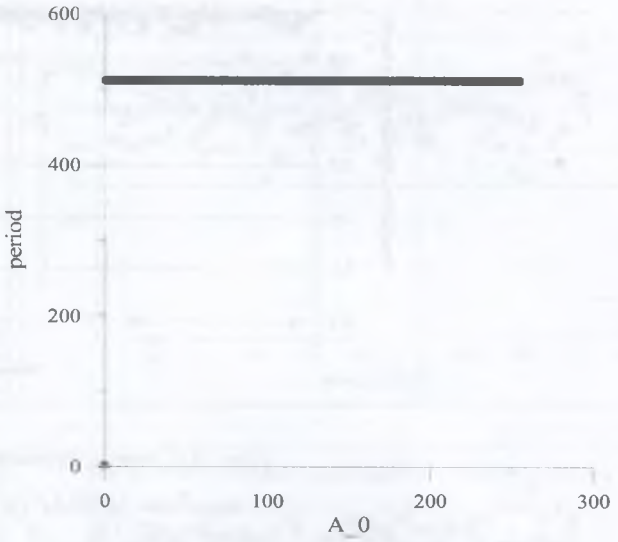


Рис. 2. Залежність періоду повторення LFSR ($F(x) = x^9 + x^4 + 1$) від початкового коду у регістрі

Для усіх значень початкового коду A_0, окрім $A\_0 = 0$, – $T_p = 2^9 - 1$. Цей факт підтверджує корисну властивість ГПВБП на основі LFSR, тобто те, що за правильного вибору твірного полінома, матриці і степеня матриці рівняння (1), період повторення ГПВБП досягає максимально можливого значення $2^n - 1$ для усіх значень початкового коду у регістрі, окрім нульового. Цим фактом ГПВБП на основі LFSR вигідно відрізняються від генераторів на основі МАГФ чи на основі *R*-блока.

Аналіз за допомогою тестів NIST наведеного генератора показав, що його статистичні характеристики не відповідають вимогам випадковості (рис. 3).

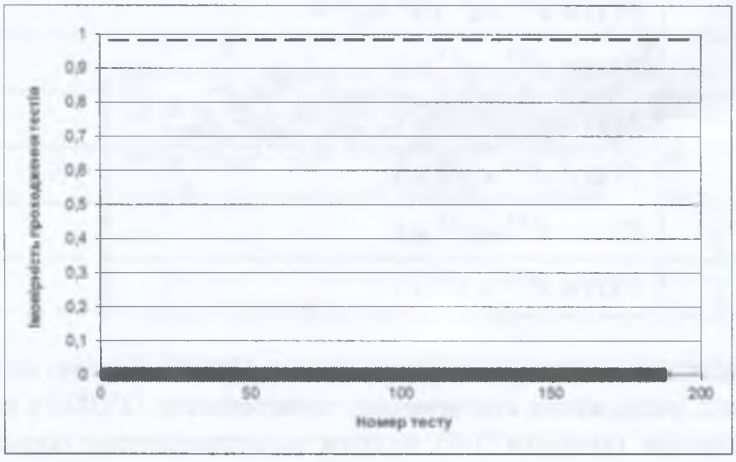


Рис. 3. Статистичний портрет ГПВБП на основі LFSR ($F(x) = x^9 + x^4 + 1$)

Далі за допомогою імітаційного моделювання і тестів NIST були досліджені характеристики генератора, реалізованого на основі твірного примітивного полінома:

$$F(x) = x^{31} + x^3 + 1, \tag{5}$$

за типу матриці T_1 і степеня матриці $r = 1$.

Його статистичний портрет, отриманий за фіксованих, в довільний спосіб заданих ночаткових установок регістра, показаний на рис. 3. Отже, цей генератор також не проходить багато тестів NIST. При цьому було зафіксовано, що період повторення вихідної послідовності генератора – $T_p > 10^9$.

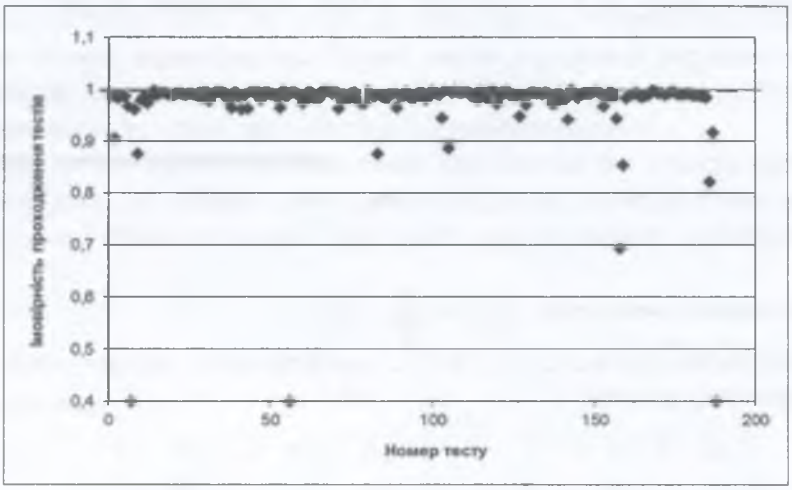


Рис. 3. Статистичний портрет ГПВБП на основі LFSR ($F(x) = x^{31} + x^3 + 1$)

Додатково здійснювалось дослідження ГПВБП побудованих на основі LFSR за поліномами, поданими у табл. 1. В усіх ГПВБП використовувалась матриця вигляду T_1, степінь матриці r = 1.

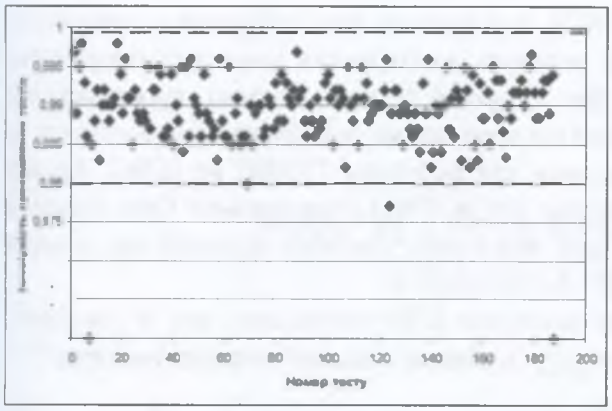
Таблиця 1

Варіанти поліномів ГПВБП

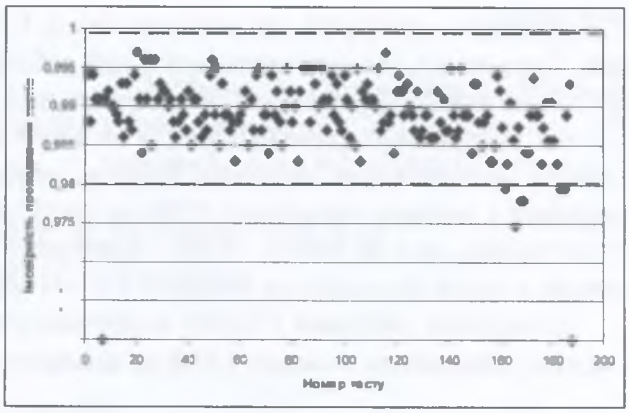
Варіант	Поліном
1	$F(x) = x^{32} + x^7 + x^6 + x^2 + 1$
2	$F(x) = x^{34} + x^8 + x^4 + x^3 + 1$
3	$F(x) = x^{135} + x^{11} + 1$
4	$F(x) = x^{137} + x^{21} + 1$
5	$F(x) = x^{140} + x^{27} + 1$
6	$F(x) = x^{151} + x^{43} + 1$
7	$F(x) = x^{177} + x^{22} + 1$

Результати дослідження статистичних характеристик ГПВБП показані на рис. 4.

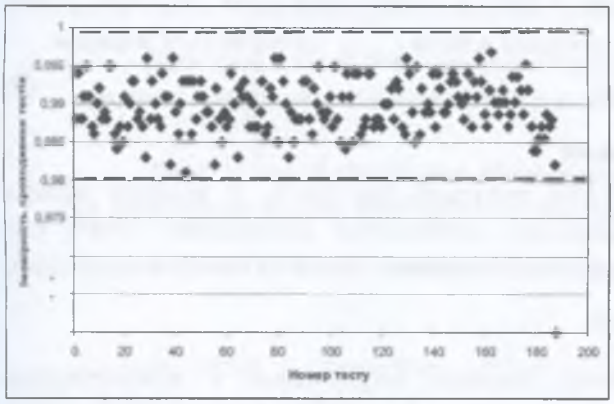
Отже, в результаті дослідження статистичних характеристик ГПВБП з'ясовано, що навіть за великих степенів поліномів (варіанти 3–7) вихідна псевдовипадкова послідовність завжди не проходить один тест, а саме: тест лінійної складності.



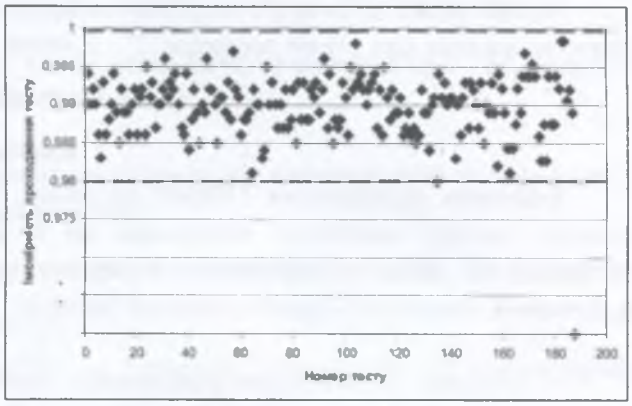
а



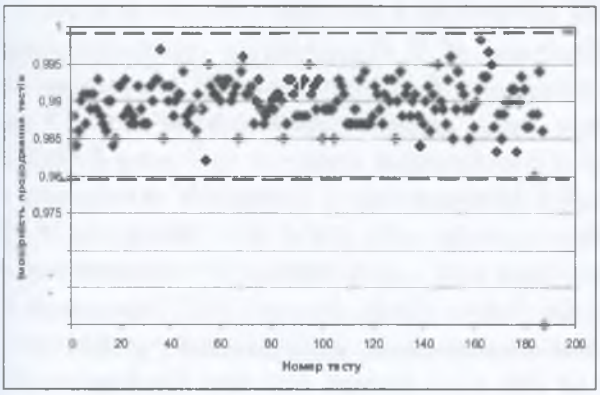
б



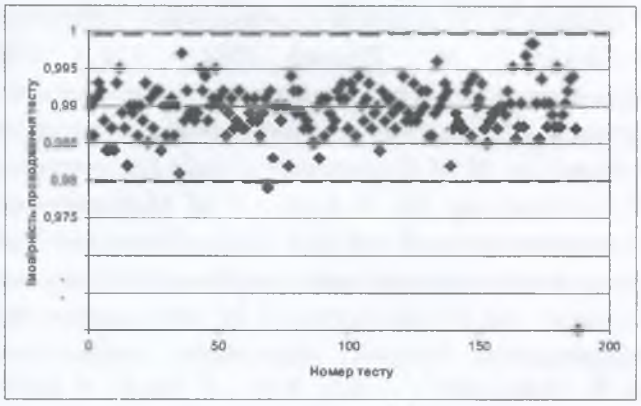
в



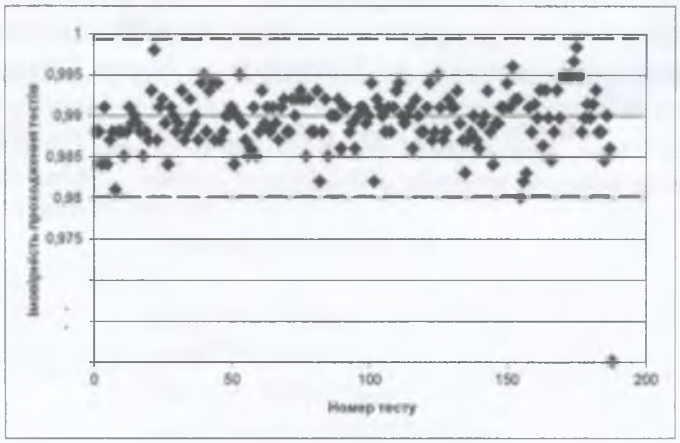
г



д



ж



з

Рис. 4. Статистичні портрети ГПВБП на основі LFSR: а – варіант 1; б – варіант 2; в – варіант 3; г – варіант 4; д – варіант 5; ж – варіант 6; з – варіант 7

Важливим фактором, що визначає якість ГПВБП, є складність його побудови – технологічність. Генератори, що розглядаються у цій роботі, належать до цифрових апаратних генераторів, тобто пристроїв, що реалізуються на елементній базі цифрової техніки, зокрема, програмованих логічних інтегральних схемах (ПЛІС). У зв'язку з цим ми пропонуємо оцінювати технологічність за кількістю елементарних цифрових комірок, необхідних для побудови ГПВБП на ПЛІС. Такими комірками у випадку організації ПЛІС за архітектурою FPGA (Field Programmable Gate Arrays) є конфігуровані логічні блоки (КЛБ), призначені для виконання логічних функцій від кількох змінних, а також функцій пам'яті [8].

Складність побудови ГПВБП визначалась за кількістю КЛБ, необхідних для їх реалізації. У випадку генератора на основі LFSR ця кількість A_{LFSR} дорівнює кількості розрядів регістра:

$$A_{LFSR} = n. \tag{6}$$

Криптографічним ключем ГПВБП на основі LFSR є початковий стан регістра. Повна множина значень цих станів дорівнює $2^n - 1$, отже, довжина ключа C_{LFSR} визначається виразом

$$C_{LFSR} = n. \tag{7}$$

Висновки

Здійснене дослідження ГПВБП на основі LFSR показало, що навіть за великих значень степенів твірних поліномів генератори не є повністю статистично безпечними. Отже, такі генератори не можна використовувати у криптографії безпосередньо, проте їх можна використати, як елементи складнішої криптографічної системи.

1. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях: учеб. пособ. / М. А. Иванова, И. В. Чугунков. – М. : НИЯУ МИФИ. 2012. – 400 с. 2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. – М. : Триумф, 2002. – 816 с. 3. Мандрона М. Н. Исследование статистических характеристик модифицированных генераторов Фибоначчи / М. Н. Мандрона, В.Н. Максымовыч // Проблемы управления и информатики : межд. наук.-техн. журн. – 2014. – № 6. – С. 28–36. 4. Mandrona M. M. Examination of multi link generators of pseudorandom sequences built using R-blocks / M. M. Mandrona, Yu. M. Kostiv, V. M. Maksymovych, O. I. Harasymchuk // Sustainable development : International journal. – Varna : Euro-Expert Ltd. – 2014. – № 18. – Pp. 110–118. 5. Мандрона М. М. Дослідження генераторів псевдовипадкових послідовностей, побудованих з використанням R-блоків / М. М. Мандрона, В. М. Максимович, Ю. Ю. Рибак, Ю. М. Костів, О. І. Гарасимчук // Інформаційна безпека: наук.-техн. журнал. Східноукраїнський національний університет ім. В. Даля. – 2013. – № 4 (12). – С. 84–92. 6. NIST SP 800-22. A Statistic Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application [Електронний ресурс]. – April 2000 // Режим доступу: http://csrc.nist.gov./publications/niatpubs//SP800-22rev1a.pdf. 7. Горбенко І. Д. Прикладна криптологія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво "Форт". 2012. – 870 с. 8. Development of a statistical security pseudorandom bit sequence generator by applying the systemic theoretical approach / Mandrona M. M., Maksymovych V. M., Harasymchuk O. I., Kostiv Yu.M. // Metallurgical and Mining Industry: scientific and technical journal. – 2016. – No. 2. – P. 96–101.

ISSN 0321-0499

№ 852
2016

ВІСНИК

НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
«ЛЬВІВСЬКА ПОЛІТЕХНІКА»

СЕРІЯ:

АВТОМАТИКА, ВИМІРЮВАННЯ ТА КЕРУВАННЯ