ДОСЛІДЖЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ГЕНЕРАТОРА ДЖИФФІ

Володимир Максимович[1], Микола Шевчук[1], Марія Мандрона[2]

1. Національний університет «Львівська політехіка», м. Львів, Україна
2. Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The article presents the results of Jiffy generator estimation with a different number of basic LFSR generators, and different degrees of their polynomials, carried out with the use of NIST statistical tests. The received results allow to optimize the generator parameters at the given parameters of the output pseudorandom sequence.

Keywords – pseudorandom generator, protection of information, pseudorandom numbers, statistic characteristics.

Генератори псевдовипадкових чисел (ГПЧ) і псевдовипадкових бітових послідовностей (ГПВБП) часто зустрічається в багатьох областях вимірювальної техніки, зокрема, при проектуванні і налагодженні потокових шифрів, та інформаційних технологій. При цьому вимоги до їх технічних характеристик відрізняються у залежності від мети їхнього застосування. Генерування псевдовипадкових послідовностей і перевірка на випадковість згенерованої послідовності є одними з найважливіших проблем сучасної криптології. У сучасних криптосистемах генератори псевдовипадкових послідовностей використовуються для створення ключової інформації і забезпечення параметрів цих систем.

Метою роботи є використання статистичних тестів Національного інституту стандартів і технологій (НІСТ) США для тестування генераторів псевдовипадкових бітових послідовностей на основі генератора Джиффі. Спрощена структурна схема генератора Джиффі наведена на рис. 1 [1]. До його складу входять три регістри LFSR1 – LFSR3 і мультиплексор MUX.

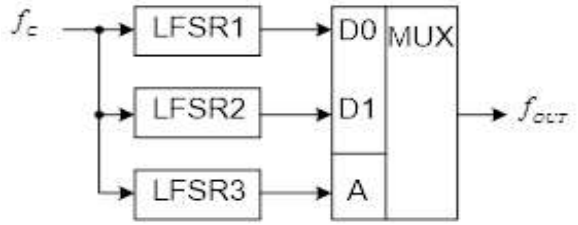

Рис. 1. Спрощена структурна схема генератора Джиффі

Генератор забезпечує перемішування двох імпульсних послідовносте з виходів LFSR1 і LFSR2 під керуванням послідовності з виходу LFSR3. У тому випадку коли значення періодів повторення вихідних послідовностей LFSR1, LFSR2, LFSR3 – T_{1p}, T_{1p}, T_{1p} попарно взаємно прості числа, період результуючою послідовності дорівнює добутку $T_J = T_{1p} \cdot T_{2p} \cdot T_{3p}$ [1].

Нами були досліджені кілька варіантів побудови генератора Джиффі, при різних структурах LFSR. Для всіх LFSR був вибраний тип матриці T_1 і степінь матриці r=1. На рис. 2-3 наведені статистичні портрети вихідної послідовності досліджуваних генераторів Джиффі, отримані при випадково вибраних фіксованих початкових установках регістрів.

Таким чином, окремі тести NIST не пройдені. При цьому, в процесі імітаційного моделювання було зафіксовано, що період повторення вихідної послідовності $T_j > 10^9$.

Отже, навіть при малих степенях поліномів, вихідна псевдовипадкова послідовність не проходить один тести NIST.

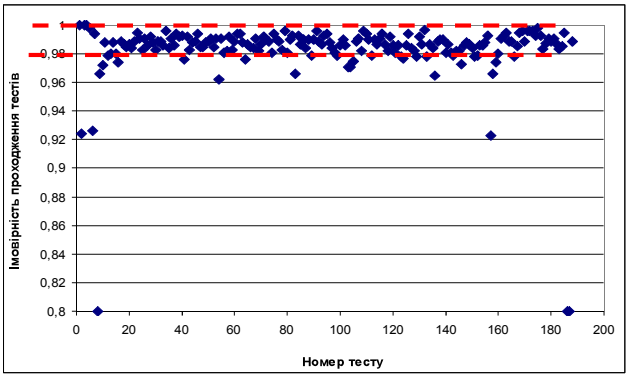

Рис. 2. Статистичний портрет генератора Джиффі (Варіант 1)

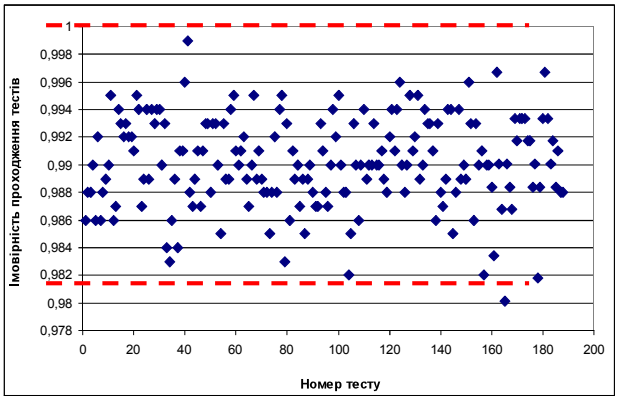

Рис. 3. Статистичний портрет генератора Джиффі (Варіант 2)

Як бачимо з рис. 3, досліджений генератор проходить усі тести NIST STS. Результати тестів знаходяться вище межі 0,98, що згідно вимог статистичного оцінювання за допомогою пакету NIST свідчить про достатню статистичну стійкість. В даному випадку усі тести NIST пройдені, і зафіксовано, що $T_j > 10^9$.

Кількість КЛБ, необхідних для побудови ГПВБП на основі генератора Джиффі, визначається сумарною кількістю розрядів усіх трьох LFSR – n_1, n_2, n_3, плюс один КЛБ для побудови мультиплексора:

$$A_{JIFFY} = n_1 + n_2 + n_3 + 1. \quad (1)$$

Криптографічним ключем ГПВБП на основі LFSR є початкові стани усіх трьох регістрів. Повна множина значень цих станів дорівнює $(2^{n_1} - 1) \cdot (2^{n_2} - 1) \cdot (2^{n_3} - 1)$, а довжина ключа визначається таким чином:

$$C_{JIFFY} = n_1 + n_2 + n_3. \quad (2)$$

Здійснене дослідження ГПВБП на основі генератора Джиффі показало, що навіть, не зважаючи на великий період повторення послідовності, при використанні малих значень степенів твірних поліномів генератори не є повністю статистично безпечними, але із збільшення степенів їх поліномів приводить до підвищення якості генератора. При зафіксованих значеннях цих поліномів ГПВБП на основі генератора Джиффі проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики і криптостійкість.

Отже, такі генератори можна використовувати у криптографії безпосередньо, проте їх можна використати, як елементи складнішої криптографічної системи.

Література

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / 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.