УДК 681.3
© О. Гарасимчук[1], З. Стрілецький[1], 2009

МОДИФІКОВАНИЙ ГЕНЕРАТОР ГОЛЛМАННА

Здійснено зміну принципу побудови генератора Голлманна з метою отримання на його виході псевдовипадкових імпульсних послідовностей, які володіли б більш кращими характеристиками. Також запропоновано вибрати групу відомих тестів для оцінки якості генераторів Голлманна.

The change of principle construction of Gollmann generator are considered in this article with the purpose of receipt on his output pseudo pulse sequences which would own the more best descriptions. Also suggested to choose the group of the known tests for the estimation of quality Gollmann generators .

1. ПОСТАНОВКА ПРОБЛЕМИ

На даний час генератори псевдовипадкових імпульсних послідовностей (ГППП) з рівномірним законом розподілу широко використовуються при моделюванні різноманітних процесів та явищ, в системах захисту інформації, а також як окремі функціональні блоки більш складних пристроїв.

Якісний ГППП, орієнтований на використання в системах захисту інформації, повинен задовольняти наступним вимогам [2]:

Криптографічна стійкість;

Хороші статистичні властивості: згенерована псевдовипадкова імпульсна послідовність не повинна відрізнятися від дійсно випадкової послідовності;

Великий період послідовності, що формується: наприклад, при шифруванні для перетворення кожного елемента вхідної послідовності необхідно використовувати свій елемент псевдовипадкової гами;

Ефективна апаратна та програмна реалізація.

Існує велика кількість різноманітних методів генерування псевдовипадкових імпульсних послідовностей, кожний з яких має свої переваги та недоліки [1-4]. Більшість з цих методів є дослідженими та ефективно застосовуються для вирішення різноманітних задач.

[1] Національний університет «Львівська політехніка»

Бажано використовувати найпростіші методи генерування псевдовипадкових імпульсних послідовностей, водночас необхідно щоб згенеровані послідовності задовольняли задані статистичні характеристики. Ще, як було сказано вище, важливим моментом є можливість реалізації ГПІП як апаратно так і програмно.

Одним з найпростіших методів генерування псевдовипадкових імпульсних послідовностей є генерування за допомогою генераторів М-послідовностей. Такі генератори ще називають генераторами псевдовипадкових чисел на лінійних послідовнісних машинах (ЛПМ), або генераторами на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (Linear Feedback Shift Register). Але безпосереднє використання генераторів М-послідовностей для отримання псевдовипадкових імпульсних послідовностей, які важко передбачити є не завжди ефективним. Тому існує багато різноманітних методів побудови ГПІП, які мають у своїй основі генератори М-послідовностей.

Одним з таких ГПІП є генератор Голлманна, який реалізується на основі кількох генераторів М-послідовностей. Властивості такого генератора є кращими порівняно з генератором М-послідовнстей, але все ж не можуть повністю задовольняти вимоги щодо випадковості, які ставляться, наприклад, при вирішенні задач захисту інформації. Тому існує питання модифікації генератора Голлманна з метою отримання на його виході імпульсних послідовностей з більшою випадковістю, та таких, які було б важко передбачити.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ

Дослідженням генераторів Голлманна, на відміну від інших типів генераторів псевдовипадкових імпульсних послідовностей присвячена невелика кількість праць. В основному дані роботи зводяться до опису принципу функціонування генераторів даного типу та рекомендацій, щодо їх побудови. А конкретні результати оцінювання послідовностей отриманих на виході таких генераторів за допомогою відомих тестів відсутні. Тому даний тип генераторів становить значний інтерес для дослідження.

Зазначимо, що існують наукові дослідження присвячені методам побудови генераторів М-послідовностей, які входять до складу генераторів Голлманна та оцінці якості їх характеристик за допомогою різноманітних оціночних та графічних тестів [2].

3. МЕТА РОБОТИ

Метою даної роботи є модифікація генератора Голлманна для отримання псевдовипадкових імпульсних послідовностей на його ви-

ході з більшою випадковістю та задовільними характеристиками порівняно з послідовностями отриманими зі стандартного генератора Голлманна. В роботі виконано оцінювання статистичних характеристик генератора Голлманна за допомогою рекомендованої групи відомих графічних та оціночних тестів.

4. МОДИФІКОВАНИЙ ГЕНЕРАТОР ГОЛЛМАНА ТА ОЦІНКА ЙОГО ЯКОСТІ

В роботі генератора Голлманна використовується принцип “stop-and-go”. Один з варіантів побудови генератора Голлманна показаний на рис. 1. В даній схемі кожен генератор М-послідовностей керує синхронізацією двох наступних генераторів. Вихід останнього генератора М-послідовностей є виходом генератора.

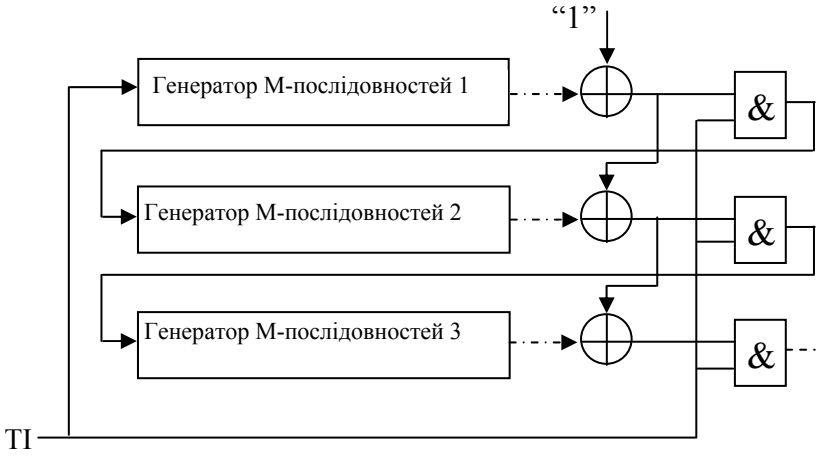

Рис. 1. Генератор Голлманна

Якщо розрядність кожного генератора дорівнює N, тоді лінійна складність системи з m генераторів М-послідовностей дорівнює

$$N(2^N - 1)^{m-1} \tag{1}$$

Концептуально даний вид генераторів є достатньо простий і може бути використаний для генерації послідовностей з великими періодами.

Відомо, що загальний вигляд рівняння генератора М-послідовностей має вигляд [2,4]

$$Q(t+1) = T^r Q(t), \tag{2}$$

де $Q(t)$ і $Q(t+1)$– стани регістра генератора в моменти часу t і t+1 відповідно (до і після приходу синхроімпульсу); T – квадратна матриця порядку N вигляду

$$T_1 = \begin{vmatrix} a_1 & a_2 & \dots & a_{N-1} & a_N \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix} \text{ або } T_2 = \begin{vmatrix} 0 & \dots & 0 & 0 & a_N \\ 1 & \dots & 0 & 0 & a_{N-1} \\ & \dots & & & \\ 0 & \dots & 1 & 0 & a_2 \\ 0 & \dots & 0 & 1 & a_1 \end{vmatrix}; \tag{3}$$

N – степінь примітивного полінома

$$\Phi(x) = \sum_{i=0}^{N} a_i x^i, \quad a_N = a_0 = 1, \quad a_j \in \{0,1\}, \quad j = \overline{1,(N-1)}, \tag{3}$$

а r – натуральне число.

У працях, присвячених опису принципів побудови генераторів Голлманна пропонується вибирати генератори М-послідовностей реалізовані лише при значенні параметра r =1.

Для дослідження різних способів побудови генератора Голлманна нами була розроблена імітаційна модель, яка дозволяє моделювати різні способи реалізації даного генератора на основі однотипних генераторів М-послідовностей, тобто кожен з m базових генераторів М-послідовностей є однотипним.

В результаті попереднього імітаційного моделювання та оцінювання якості генератора Голлманна ми вибрати твірний поліном $\Phi(x) = 1 \oplus x^2 + x^5$. Кількість m таких генераторів М-послідовностей при побудові генератора Голлманна вирішено вибрати рівною 5.

Суть нашого дослідження полягає в тому, що ми вирішили використовувати генератори М-послідовностей змінюючи степінь r матриці T_1. Як показали дослідження [4], зміна r впливає на якість псевдовипадкової імпульсної послідовності на виході генератора М-послідовностей. Тому вирішено перевірити, чи це вплине позитивно на якість послідовності отриманої з виходу генератора Голлманна.

При оцінюванні якості генератора Голлманна неможливо спиратись лише на один тест чи на тести однієї групи. Тому при виконанні даної роботи нами було прийняте рішення про використання як графічних так і оціночних тестів, причому не в одному примірнику.

Попередньо проаналізувавши різні графічні та оціночні тести нами було запропоновано вибрати для подальшої роботи відомі 2 графічні тести (розподіл на площині та гістограма розподілу елементів) та 4 оціночні тести (частотний тест, тест дирок, перевірка перестановок та тест посимвольної перевірки).

Всі оціночні тести були вибрані з різних наборів статистичних тестів, а саме - з підбірки тестів Д.Кнута вибрано тест перевірки перестановок, зі статистичних тестів НІСТ вибрано частотний монобітний тест та тест дирок і ще один оціночний тест, який не увійшов у згадані вище підбірки – тест посимвольної перевірки.

Не будемо вдаватись в детальний опис та основні принципи реалізації цих тестів, лише зазначимо що деякі з них призначені для перевірки на рівномірність псевдовипадкової двійкової послідовності (частотний монобітний тест та тест дирок), а деякі для тестування та перевірки на рівномірність послідовності к-розрядних чисел довжини l (тест перестановок та тест посимвольної перевірки).

На рис. 2 наведені результати оцінювання за допомогою тесту розподілу на площині псевдовипадкових чисел на виході генератора Голлманна залежно від різних значень r (де x, x_pop – відповідно чергове та попереднє значення псевдовипадкового числа). Як видно з даного рисунку, змінюючи значення r ми отримуємо більш випадкову послідовність на виході генератора Голлманна. Тобто, ми за допомогою графічного тесту переконались, що модифікуючи базові генератори М-послідовностей ми отримали на виході генератора Голлманна псевдовипадкову послідовність з кращими статистичними характеристиками. Також аналогічне підтвердження було отримане при оцінюванні гістограм розподілу елементів на виході генератора Голлманна при відповідних змінах параметра r.

Для ефективнішого оцінювання виконаємо кілька оціночних тестів. Результати такого тестування наведені в таблиці 1. Як видно з даної таблиці, ми ще раз отримали підтвердження того, що запропоновані нами зміни покращили статистичні характеристики генератора Голлманна. Важливою особливістю, яку видно з результатів проведеного тестування є те, що використання одного тесту не може бути ефективним при оцінюванні псевдовипадкових імпульсних послідовностей, оскільки одна і та ж послідовність може деякі тести проходити повністю, а інші не проходити ніколи. Отже, загальний висновок про якість послідовності можна робити лише на основі тестування кількома різними тестами.

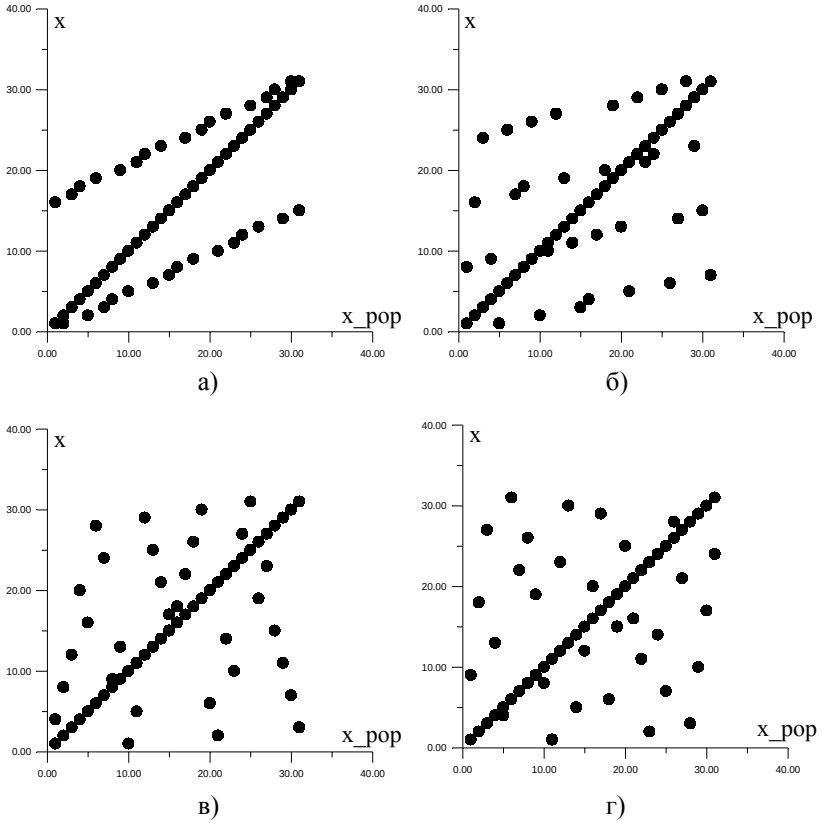

Рис. 2. Розподіл на площині псевдовипадкових чисел на виході генератора Голлманна: а) r=1; б) r=2; в) r=3; г) r=5.

Таблиця 1.

Результати тестування генератора Голлманна
за допомогою оціночних тестів

	Вид тесту			
Значення r	Тест дирок	Частотний монобітний тест	Перевірка перестановок	Посимвольна перевірка
1	–	+	–	+
2	+	+	–	+
3	+	+	–	+
4	+	+	–	+
5	+	+	–	+

Варто також зауважити, що для генераторів М-послідовностей при побудові генераторів Голлманна параметр r необхідно вибирати невеликим, щоб не ускладнювати принципову схему. Достатньо вибирати його в межах від 3 до 5. Саме в таких межах ми отримаємо покращені характеристики вихідної імпульсної послідовності, а сама принципова схема реалізації генератора Голлманна незначно ускладниться.

5. ВИСНОВКИ

Як видно з результатів досліджень наведених на рис. 2 та у таблиці 1 запропоновані нами зміни в принципі побудови генератора Голлманна покращують його статистичні характеристики, що значно розширює сферу їх застосування. Оцінка якості генераторів Голлманан на основі групи тестів є ефективнішою, ніж на основі лише одного тесту.

1. Гундарь, К. Ю. Защита информации в компьютерных системах [Текст] / Гундарь, К. Ю., Гундарь, А. Ю., Янишевский, Д. А.// К.: "Корнейчук", 2000. – 152 с. 2. Иванов, М. А., Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / Иванов, М. А., Чугунков, И. В. // М.: КУДИЦ – ОБРАЗ, 2003. – 240 с. – (СКБ – специалисту по компьютерной безопасности). 3. Гарасимчук, О. І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості [Текст] / Гарасимчук, О. І., Максимович, В. М., // "Захист інформації". – м.Київ, 2002, 7 стор. 4. Гарасимчук, О. І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей [Текст] / Гарасимчук, О. І., Максимович, В. М. // Вісник Національного університету "Львівська політехніка" "Комп'ютерні науки та інформаційні технології", – 2004. – №521 – С. 17-23.