УДК 681.3

О.І. Гарасимчук, Ю.М. Костів, Т.Г. Паршенко

Національний університет "Львівська політехніка", Львів

ОЦІНКА ЯКОСТІ ГЕНЕРАТОРА ГОЛЛМАННА, РЕАЛІЗОВАНОГО НА ОСНОВІ МОДИФІКОВАНИХ ГЕНЕРАТОРІВ М-ПОСЛІДОВНОСТЕЙ

В даній роботі за допомогою імітаційного моделювання досліджені характеристики псевдовипадкової імпульсної послідовності на виході генератора Голлманна, реалізованого на основі різних типів базових генераторів М-послідовностей. Дослідження проводились в результаті зміни кількості базових генераторів М-послідовностей, основних принципів їх реалізації, та послідовності включення в загальну схему генератора. Оцінка ефективності здійснювалась на основі обраної групи відомих статистичних тестів.

Ключові слова: *псевдовипадкова імпульсна послідовність, генератор Голлманна, генератор М-послідовностей, статистичні тести.*

Вступ

Постановка проблеми. У зв'язку зі стрімким розвитком засобів обчислювальної і вимірювальної техніки, а також із впровадженням новітніх технологій значно розширилась сфера застосування генераторів випадкових і псевдовипадкових імпульсних послідовностей. А це в свою чергу ставить нові вимоги до їх проектування та методів оцінки якості.

На даний час, генератори випадкових і псевдовипадкових імпульсних послідовностей широко використовуються:

- системах захисту інформації – для шифрування, розшифрування та генерації ключів, генерування шуму, цифрових підписів, протоколів безпеки і т.д.;
- в імітаційному моделюванні – для фізичних, математичних, хімічних, економічних та медичних досліджень, а також в моделюванні військових дій;
- у вимірювальній техніці – як окремі функціональні блоки вимірювальних приладів або для їхнього тестування;
- при розробці комп'ютерних ігор.

Основними вимогами, що стоять перед розробниками ГПІП є наступні:

- простота апаратної або програмної реалізації;
- максимальна швидкодія;
- максимальна наближеність послідовності отриманої на виході генератора до теоретичного закону розподілу;
- можливість керування вихідними параметрами;
- можливість роботи ГПІП в широкому діапазоні частот;
- можливість швидкого переналагодження його роботи в залежності від вибору вихідних параметрів.

Існує велика кількість різноманітних методів та принципів генерування псевдовипадкових імпульсних послідовностей, кожний з яких має свої переваги та недоліки [1 – 5]. Більшість з цих методів ефективно застосовуються для вирішення різноманітних задач.

Перед розробниками ГПІП стоїть непросте завдання, щодо поєднання використання найпростіших методів генерування псевдовипадкових імпульсних послідовностей, та одночасного забезпечення заданих статистичних характеристик на виходах таких генераторів. Ще, як було згадано вище, важливим моментом є можливість реалізації ГПІП як апаратно так і програмно.

Одними з найпростіших генераторів псевдовипадкових послідовностей є генератори М-послідовностей (їх 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). Такі генератори знайшли широке використання в різних галузях науки та техніки. Але безпосереднє використання генераторів М-послідовностей в більшості випадків є не завжди ефективним, оскільки послідовність на їх виході досить легко передбачити. Тому існує багато різноманітних методів побудови ГПІП, які базуються на використанні генераторів М-послідовностей.

До таких генераторів, наприклад, можна віднести генератор Голлманна, який реалізується на основі кількох генераторів М-послідовностей, що взаємопов'язані.

Властивості такого генератора при правильній реалізації є кращими в порівнянні з генератором М-послідовностей, але все ж не завжди можуть повністю задовольняти вимоги, щодо випадковості, які ставляться, наприклад, при вирішенні задач захисту інформації.

Для покращення характеристик генератора Голлманна доцільно спробувати модифікувати базові генератори М-послідовностей та вибрати оптимальні їх параметри, які задовольняли б певні статистичні критерії.

Аналіз останніх досліджень. На даний час, генератори Голлманна є малодослідженими. В основному всі роботи які присвячені даному типу генераторів зводяться до рекомендацій щодо побудови та формального опису принципів функціонування таких генераторів. А конкретні результати оцінювання послідовностей отриманих на їх виході за допомогою відомих тестів, порівняльний аналіз таких генераторів є відсутніми. Тому, великий інтерес являє собою оцінка його якості при різних початкових параметрах, а також дослідження його на можливість використання в системах захисту інформації.

Метою даної роботи є визначення впливу вихідних параметрів базових генераторів М-послідовностей та способів включення таких базових генераторів на псевдовипадкові імпульсні послідовності на виході генератора Голлманна та вибір групи тестів для ефективної оцінки статистичних характеристик згенерованих послідовностей.

Реалізація генератора Голлманна на основі генераторів М-послідовностей та оцінка їх якості

Принцип реалізації генератора Голлманна є досить простий – в його роботі використовується принцип “stop-and-go” (рис. 1). В даній схемі кожен генератор М-послідовностей керує синхронізацією наступних генераторів. Вихід останнього генератора М-послідовностей є виходом генератора.

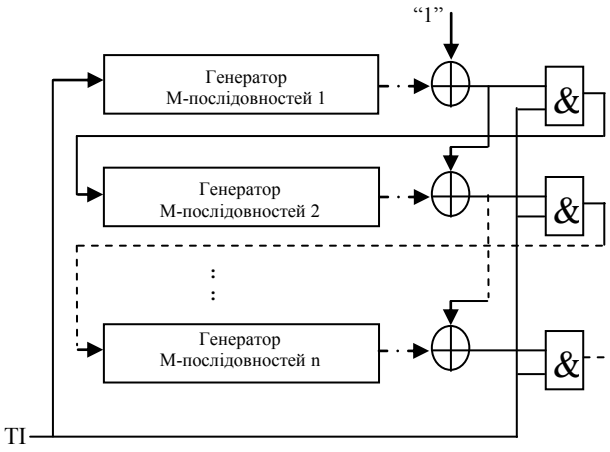

Рис. 1. Генератор Голлманна

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

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

Криптографи радять використовувати $m \geq 15$, а при рівних значеннях mN віддавати перевагу варіанту з більшим числом коротких LFSR, а не варіанту з меншим числом довгих LFSR.

Концептуально даний вид генераторів є достатньо простий і може бути використаний для генерації псевдовипадкових послідовностей з величезними періодами, великими лінійними складностями.

Опис принципів побудови генераторів М-послідовностей в даній роботі наведений не буде, оскільки він є відомим і детально наведений у великій кількості літератури. Як відомо [4] генератори М-послідовностей володіють кращими статистичними характеристиками при зміні складності їх реалізації, а саме при модифікації їх таким чином, щоб на виході таких ГППП отримувати послідовності, які були б більш випадковими (зміна параметра r – степеня до якого підноситься матриця на основі якої реалізується генератор М-послідовностей).

У працях, які присвячені опису принципів побудови генератора Голлманна пропонується вибирати в якості базових лише генератори М-послідовностей реалізовані при значенні параметра r =1.

Для дослідження різних способів побудови генератора Голлманна нами була розроблена імітаційна модель такого генератора на мові C#, яка дозволяє моделювати різні способи реалізації даного генератора на основі однотипних генераторів М-послідовностей (як це переважно рекомендують в літературі), тобто кожен з m базових генераторів М-послідовностей є однотипним, а також на основі різних базових генераторів М-послідовностей. Також в програмі передбачена оцінка ефективності згенерованих псевдовипадкових послідовностей за допомогою статистичних тестів.

Оцінку якості будь-якого ГППП неможливо виконувати на основі лише якогось одного тесту, тому виконуючи наші дослідження ми обрали кілька відомих оціночних тестів з різних наборів статистичних тестів., а саме з підбірки тестів Д.Кнута та зі статистичних тестів НІСТ [2]. В детальний опис цих тестів ми вдаватись не будемо, оскільки вони є досить відомими. Введемо їх позначення, для подальшого використання при описі результатів дослідження:

1) частотний (монобітний) тест;
2) частотний тест в підпослідовностях;
3) тест "дірок";
4) тест блоків в під послідовностях;
5) тест перевірки серій;
6) тест перевірки апроксимованої ентропії.

Суть нашого дослідження полягає в тому, що ми вирішили використовувати генератори М-послідовностей змінюючи степінь r матриці T_1 на основі якої вони реалізуються, оскільки, як показали дослідження [4], така зміна ефективно 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. Окрім того ми вирішили перевірити як на якість вихідної імпульсної послідовності впли-

вають твірні поліноми на основі яких реалізуються генератори М-послідовностей та комбінації включення таких базових генераторів.

На початковому етапі наших досліджень ми вирішили з'ясувати як впливає кількість базових генераторів М-послідовностей на якість згенерованої послідовності на виході генератора Голлманна. Для цього ми вибрали в якості базових генератори реалізовані на основі твірного поліному

$$\Phi\ x\ = x^4 + x^3 + 1.$$

Кількість m таких генераторів М-послідовностей при побудові генератора Голлманна вирішено вибрати 5,7,9. Значення степеня r=1 (табл. 1).

Таблиця 1

Результати оцінювання
генератора Голлманна при зміні
кількості базових однотипних генераторів

№ з/п	m	Тип тесту					
		1	2	3	4	5	6
1.	5	+	–	–	+	+	–
2.	7	+	–	–	+	+	+
3.	9	+	–	+	+	+	+

В даній таблиці "+"означає, що тест пройдено, а "–" означає, що тест не пройдено.

Як видно з результатів, наведених в табл. 1, при збільшенні кількості однотипних базових генераторів зростає якість псевдовипадкової послідовності на виході генератора Голлманна.

Далі нами було оцінено влив різних твірних поліномів та значень r на якість вихідної імпульсної послідовності. Для цього було прийнято рішення проаналізувати комбінації з трьох твірних поліномів різного степеня. Генератори реалізовані на основі цих твірних поліномів відповідно позначимо:

а) $\Phi\ x\ = x^8 + x^4 + x^3 + x^2 + 1$;

б) $\Phi\ x\ = x^7 + x + 1$;

в) $\Phi\ x\ = x^6 + x + 1$.

Спочатку було вивчено вплив послідовності використання різних базових генераторів реалізованих на основі цих твірних поліномів. Оскільки кожен попередній генератор керує роботою наступного і в залежності від свого стану може запускати чи не запускати наступний генератор, то цікаво як вплине період повторення імпульсної послідовності на виході кожного базового генератора (який залежить від степеня твірного поліному) на якість послідовності отриманої на виході генератора Голлманна (табл. 2).

Проаналізувавши результати наведені в табл. 2 можна зробити висновок, що при побудові генератора Голлманна бажано дотримуватись такого принципу, щоб базові генератори М-послідовностей розташовувались в порядку спадання степеня їх твірного поліному, оскільки це значно покращує якість імпульсної псевдовипадкової послідовності на виході генератора Голлманна.

Таблиця 2

Визначення впливу
розрядності базових генераторів
М-послідовностей на якість генератора Голлманна

№ п/п	Послідовність базових генераторів			Тип тесту					
				1	2	3	4	5	6
1.	**а)**	**б)**	**в)**	+	–	+	+	+	+
2.	а)	в)	б)	+	–	+	–	+	+
3.	б)	а)	в)	+	–	+	–	+	+
4.	б)	в)	а)	+	–	+	–	+	–
5.	в)	а)	б)	+	–	–	–	+	–
6.	в)	б)	а)	+	–	–	–	+	–

Далі дослідження проводились для аналізу змін якості вихідної послідовності генератора в залежності від значення степеня r.

Для цього було обрано наступну послідовність включення базових генераторів: а) – в) – б).

Результати, наведені в табл. 3, вказують на те, що якість генератора Голлманна буде покращуватись за умови ускладнення роботи базових генераторів М-послідовностей, які стоять першими та керують роботою наступних базових генераторів. Це можна пояснити тим, що таким чином вноситься більша випадковість і умови запуску кожного наступного генератора є більш випадковими і зміна станів наступних генераторів буде відбуватися частіше.

Таблиця 3

Результати оцінювання генератора Голлманна
в залежності від зміни степеня r

№ п/п	Значення *r*			Тип тесту					
	а)	в)	б)	1	2	3	4	5	6
1.	1	1	1	+	–	+	–	+	+
2.	4	1	1	+	–	+	+	+	–
3.	1	4	1	+	–	–	–	+	–
4.	1	1	4	+	–	+	–	+	–
5.	4	4	1	+	–	+	–	+	+
6.	4	1	4	+	–	+	+	+	+
7.	4	4	4	+	–	+	–	+	+

Наведені в табл. 1 – 3 результати були також підтверджені імітаційним моделюванням та оцінкою якості генераторів Голлманна за умови вибору базо-

вих генераторів реалізованих на інших твірних поліномах, та за умов вибору такого самого степеня r як в даних дослідженнях і таких самих принципів розташування даних генераторів.

Також дуже важливою особливістю, яку видно в результаті проведеного тестування та на яку варто звернути особливу увагу є те, що використання одного тесту не може бути ефективним (гарантувати 100% правильного результату) 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, що бажано вибирати з різних груп оціночних чи графічних тестів.

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 ускладниться незначно.

Висновки

Як видно з результатів досліджень, наведених в табл. 1 – 3, запропоновані нами підходи до реалізації генератора Голлманна, вибору початкових його параметрів, принципів включення базових генераторів М-послідовностей, та способів їх реалізації покращують статистичні характеристики псевдовипадкової послідовності на його виході, що значно розширює сферу застосування таких генераторів та робить можливим їх застосування в системах захисту інформації.

Оцінка якості генераторів Голлманна на основі групи тестів є більш ефективною, чим на основі лише одного тесту.

Перспективами подальших досліджень в даному напрямку може бути використання в якості базових генераторів М-послідовностей генераторів реалізованих на основі примітивних поліномів великого степеня, та збільшення кількості таких базових генераторів.

Також варто реалізувати такі генератори на програмованих логічних інтегральних схемах з метою дослідження їх часових та частотних характеристик.

Список літератури

1. Гундарь К.Ю. Защита информации в компьютерных системах [Текст] / К.Ю. Гундарь, А.Ю. Гундарь, Д.А. Янишевский. – К.: "Корнейчук", 2000. – 152 с.

2. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М.А.Иванов, И.В. Чугунков // 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] / О.І. Гарасимчук, В.М. Максимович // Захист інформації. – К., 2002. – 7 с.

4. Гарасимчук О.І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей [Текст] / О.І. Гарасимчук, В.М. Максимович // Вісник Національного університету "Львівська політехніка". Комп'ютерні науки та інформаційні технології. – 2004. – № 521. – С. 17-23.

5. Гарасимчук О.І. Модифікований генератор Голлманна [Текст] / О.І. Гарасимчук, З.М. Стрілецький // Комп'ютерні технології друкарства: збірник наукових праць. – 2009. – № 22 – С. 64-70.

Надійшла до редколегії 15.09.2010

Рецензент: д-р техн. наук, проф. В.М. Максимович, Національний університет "Львівська політехніка", Львів.

ОЦЕНКА КАЧЕСТВА ГЕНЕРАТОРА ГОЛЛМАННА, РЕАЛИЗОВАННОГО НА ОСНОВЕ МОДИФИЦИРОВАННЫХ ГЕНЕРАТОРОВ М-ПОСЛЕДОВАТЕЛЬНОСТЕЙ

О.И. Гарасимчук, Ю.Н. Костив, Т.Г. Паршенко

Рассматриваются принципы построения генераторов Голлманна на базе разных способов реализации базовых генераторов М-последовательностей. Выполнена оценка качества псевдослучайных последовательностей на выходе генератора Голлманна при помощи выбранной группы статистических тестов.

Ключевые слова: *псевдослучайная импульсная последовательность, генератор Голлманна, генератор М-последовательностей, статистические тесты.*

EVALUATION OF THE QUALITY OF THE GENERATOR GOLLMANNA IMPLEMENTE BASED ON MODIFIED GENERATORS M-SEQUENCE

O.I. Garasymchuk, Y.M. Kostiv, T.G. Parshenko

Considered the principles of constructing generators Gollmann based on different ways to implement basic generators M-sequence. Maked the estimation of the quality of pseudorandom sequences generator output Gollmann by selected group of statistical tests.

Keywords: *pseudocasual impulsive sequence, generator of Gollmann, generator of Mcodes-sequences, statistical tests.*