УДК 621.317.083

Ю.М. Костів[1], В.М. Максимович[1], О.І. Гарасимчук[2], Я.Р. Совин[2], М.М. Мандрона[1]
[1]Кафедра безпеки інформаційних технологій,
[2]Кафедра захисту інформації,
Національного університету "Львівська політехніка"

ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ПАРАМЕТРІВ ГЕНЕРАТОРА ГОЛЛМАННА ЗА ДОПОМОГОЮ СТАТИСТИЧНИХ ТЕСТІВ NIST

Annotation

The article presents the results of Gollmann 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 pulse sequence.

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

Анотація

В статті представлені результати дослідження генератора Голлманна при різній кількості базових генераторів М-послідовностей і різній степені їх поліномів, що проводилось з використанням статистичних тестів NIST. Отримані результати дозволяють оптимізувати параметри генератора при заданих параметрах вихідної імпульсної послідовності.

Ключові слова – генератори псевдовипадкових чисел, захист інформації, псевдовипадкові числа, статистичні характеристики.

Вступ

Псевдовипадкова послідовність – це послідовність, що виглядає як випадкова, але насправді має скінченний період повторення.

Тому, при проектуванні генераторів псевдовипадкових послідовностей (ГПВП), необхідно зважати на найважливішу характеристику генератора – довжину періоду, після якого числа або почнуть знову повторюватися, або їх буде можливо передбачити. Добре згенерована псевдовипадкова послідовність практично не відрізняється від істинно випадкової.

Однією з переваг ГПВП є те, що на виходах таких генераторів ми отримуємо результати, які можна повторити нескінченну кількість разів, при заданні однакових початкових умов та параметрів, що є досить зручно, особливо в процесі статистичного моделювання.

Зважаючи на швидкий розвиток засобів обчислювальної і вимірювальної техніки, а також із впровадженням новітніх технологій значно розширюється сфера застосування генераторів випадкових і псевдовипадкових послідовностей, а тому висуваються нові вимоги до їх проектування та методів оцінки якості.

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

- в 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;
- як аналогові або цифрові джерела шуму;
- як коди для радіолокаційних систем, в яких відповідний сигнал взаємно корелюється з бітовою послідовністю, що передається;

- при розробці комп'ютерних ігор.

При проектуванні та реалізації ГПВП необхідно дотримуватись наступних загальноприйнятих вимог:

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

Якщо такий генератор буде використовуватися в системах захисту інформації (а такі генератори часто є важливою ланкою в забезпеченні інформаційної безпеки, зокрема в криптографії), то до нього висувається ще ряд додаткових вимог, що будуть більш жорсткими у порівнянні з вимогами до генераторів, що використовуються в інших галузях. Виконання таких вимог в першу чергу дозволяє виявити генератори, що наперед задовольняють вимоги конкретної криптографічної задачі.

Найбільшою проблемою практично будь-якого ГПВП є те, що при визначених початкових умовах вони дають передбачувані результати та кореляційні залежності. А це якраз те, що очікують від псевдовипадкових послідовностей криптоаналітики, для здійснення ефективної атаки на криптосистему, де ці генератори застосовуються. Тому, якщо такий генератор буде застосовуватися наприклад в криптографічних додатках, то по-перше він повинен проходити статистичні тести на випадковість, а по-друге він повинен зберігати непередбачуваність, навіть якщо частина вихідного або поточного стану стане відомою для криптоаналітика.

Ще одна проблема полягає в тому, що не існує базису на основі якого можна зробити висновок, що гамма конкретного генератора є непередбачуваною. На даний час в світі немає ще універсальних та таких, що на практиці перевіряються критеріїв, які б дозволяли стверджувати це. Невідомою є також і загальна теорія криптоаналізу, що могла б бути застосована для такого доведення, за виключенням зростаючої кількості конкретних способів аналізу, вироблених для різних практичних цілей. Інтуїтивно випадковість сприймається як непередбачуваність, а для того щоб вважати гамму випадковою, як мінімум необхідно, щоб її період був дуже великим, а різноманітні комбінації біт визначеної довжини розподілялися рівномірно по всій її довжині [1].

На даний час розроблена велика кількість різноманітних методів та принципів генерування псевдовипадкових послідовностей, кожний з яких має свої переваги та недоліки [2-6], та ефективно застосовуються для вирішення різноманітних задач.

При виборі того чи іншого типу ГПВП, окрім виконання перелічених вище вимог до послідовностей на його виході, бажано поєднувати використання найпростіших методів генерування псевдовипадкових послідовностей, та одночасного забезпечення заданих статистичних характеристик на виходах таких генераторів. Також бажано передбачити можливість реалізації ГПВП, як апаратно так і програмно.

Одним з найбільш простих в реалізації та найбільш поширеніших є спосіб генерування псевдовипадкових послідовностей на основі регістрів зсуву. Такі генератори називають генератори М-послідовностей (генератори псевдовипадкових чисел на лінійних послідовнісних машинах (ЛПМ), або генераторами на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (Linear Feedback Shift Register). Незважаючи на свою простоту та те, що на їх виході отримуються послідовності, які в основному є прогнозовані та передбачувані, такі генератори знайшли широке використання в різних галузях науки та техніки.

Але безпосереднє використання генераторів М-послідовностей зважаючи на згадані недоліки в більшості випадків є не завжди ефективним, оскільки послідовність на їх виході досить легко передбачити, що особливо непридатно для їх безпосереднього застосування при вирішенні задач

захисту інформації. Тому існує багато різноманітних методів побудови більш складних ГПІП, які базуються на використанні генераторів М-послідовностей.

Серед таких методів варто звернути увагу на 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. Генератори Голлманна широко використовуються у тих же сферах, що описані вище для ГПВЧ, а також можуть прямо чи опосередковано застосовуватись при вирішення задач захисту інформації. Практичним дослідженням генераторів Голлманна, на відміну від інших типів генераторів (зокрема й генераторів М-послідовностей, що входять до їх складу) присвячена відносно невелика кількість праць, що в основному зводяться до опису принципів функціонування генераторів даного типу та рекомендацій щодо їх побудови.

Тому виникає задача, що полягає у покращенні характеристик генератора Голлманна з метою отримання на його виході псевдовипадкових послідовностей, що прямо чи опосередковано можна було б застосовувати при вирішенні задач захисту інформації. Тому доцільно спробувати модифікувати базові генератори М-послідовностей та вибрати оптимальні їх параметри, які задовольняли б певні статистичні критерії.

Для того щоб робити висновок про можливість застосування того чи іншого ГПВП для вирішення конкретних задач потрібно виконати оцінювання його якості та надійності. Тестування генераторів псевдовипадкових послідовностей, особливо тих, що використовуються в криптографічних додатках є актуальною задачею як в практичному так і в теоретичному плані. Незважаючи на значні напрацювання в цій області розробники все таки потребують зручного інструментарію, що здатний надати допустиму метрику, яка дозволить достатньо чітко дослідити степінь випадковості послідовності на виході генератора, а також забезпечить розробників достатнім об'ємом інформації для прийняття рішення відносно якості ГПВП.

На даний час існують та широко використовується достатньо велика кількість різних типів ГПВП, а набір та методику тестування кожного з них, як правило пропонував сам розробник генератора [7]. Тому обставини складалися так, що було важко об'єктивно порівняти різні генератори на основі спільних критеріїв. Єдиним можливим виходом з такого становища є використання деякого стандартного набору статистичних тестів, що об'єднані певною спільною методикою розрахунку необхідних показників ефективності ГПВП та прийняття рішення про випадковість послідовності, що тестується. Тому науковці почали вести інтенсивну роботу в цьому напрямку, що привела до визначення двох основних груп критеріїв. Перша така група пов'язана з пошуком закономірностей, що дозволяють відновити шифровану послідовність по відносно невеликій кількості матеріалу. При цьому висуваються вимоги по відсутності в псевдовипадковій послідовності відносно простих міжзнакових залежностей. Друга група критеріїв базується на оцінці статистичних властивостей послідовності, а саме чи є в послідовності, що досліджується який-небудь частотний дисбаланс, що дозволяє аналітику передбачити значення наступного біту із ймовірністю більше чим 0.5. Також повинна забезпечуватися найбільша близькість властивостей псевдовипадкової послідовності до дійсно випадкової послідовності. Дані дві групи критеріїв складають основу системного підходу до розробки тестів, що призначені для оцінки якості псевдовипадкових послідовностей.

На сьогоднішній день для тестування псевдовипадкових послідовностей розроблено кілька програмних продуктів, що містять комплекси тестів для перевірки різних статистичних властивостей, такі як тести Д. Кнута, DIEHART, CRYPT-S, FIPS, але найвідомішим серед яких є набір статистичний тестів NIST [8,9].

Мета роботи

Проведення оцінювання генераторів Голлманна за допомогою пакету статистичних тестів NIST з метою визначення впливу параметрів їх структурних елементів на якість генератора.

Генератор Голлманна та результати його досліджень

Генератор Голлманна складається з кількох послідовно з'єднаних генераторів М-послідовностей (регістрів зсуву), тактування кожного з яких керується попереднім генератором (рис. 1). Вихід останнього генератора М-послідовностей є виходом генератора.

Якщо розрядність кожного генератора дорівнює *N*, тоді лінійна складність системи з *m* генераторів М-послідовностей дорівнює [3]

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

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.

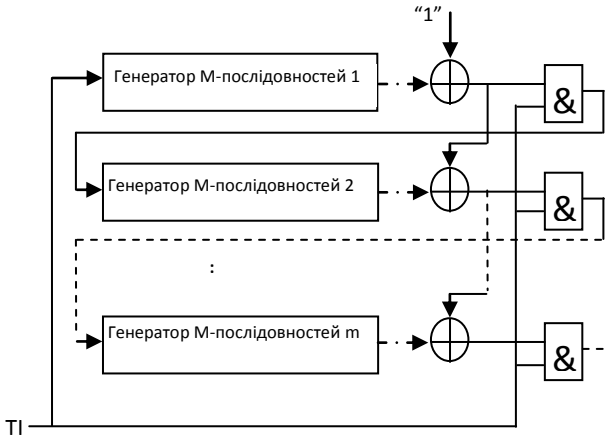

Рис.1. Генератор Голлманна

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

Такі генератори є чутливими до розкриття, що називається закривання (look-in), що являє собою метод за допомогою якого спочатку криптоаналітик відновлює вхід останнього регістра зсуву в каскаді, а потім взламує весь каскад регістр за регістром. В деяких випадках це становить суттєву проблему та зменшує ефективну довжину ключа алгоритму, але для мінімізації можливості такого розкриття можна застосувати ряд визначених мір.

Рівняння генератора М-послідовностей має вигляд [3]:

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

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

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

N – степінь примітивного полінома

$$\Phi(x) = \sum_{i=0}^{N} a_i x^i, \quad a_N = a_0 = 1, \quad a_j \in \{0,1\}, \quad j = \overline{1,(N-1)}, \tag{4}$$

r – натуральне число.

Детальні принципи реалізації генераторів М-послідовностей в даній роботі наведені не будуть, оскільки вони є відомими і детально наведені у великій кількості літератури. Доведено [5], що кращі статистичні характеристики мають ті генератори М-послідовностей, які є модифіковані (мають складнішу реалізацію). Для дослідження та оцінки якості генераторів Голлманна ми вирішили змінювати розрядність базових генераторів М-послідовностей, а також змінювати кількість таких генераторів. Оцінювання якості генератора виконаємо за допомогою пакету статистичних тестів NIST. Результати такого оцінювання генератора Голлманна, на даний час, в літературі відсутні. Для цього нами була розроблена імітаційна модель такого генератора на мові Delphi, яка дозволяє одержувати вихідні послідовності в залежності від зміни згаданих вище параметрів.

Статистичні тести NIST – пакет статистичних тестів, який розроблений в 1999 р. лабораторією інформаційних технологій (Information Technology Laboratory), що є головною організацією Національного Інституту Стандартів і Технологій США (NIST) [10]. Фахівцями NIST запропонована методика проведення статистичного тестування генераторів псевдовипадкових чисел, що орієнтовані на застосування в системах захисту інформації – зокрема в криптографії. Тому даний пакет використовуються для визначення якісних та кількісних ознак випадковості послідовності чисел, що є необхідно для криптографів та криптоаналітиків.

Пакет NIST STS включає в себе 15 статистичних тестів, які розроблені для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, що генеруються ГПВП. Кожен з даних тестів спрямований на виявлення різноманітних дефектів випадковості.

Результати кожного статистичного тесту повинні тлумачитись з певною обережністю і застереженням, щоб уникнути неправильних висновків про досліджуваний генератор.

Базовим принципом тестування за допомогою статистичних тестів NIST є перевірка певної нульової гіпотези H_0 про те, що послідовність, яка перевіряється є випадковою. З цією нульовою гіпотезою пов'язана альтернативна гіпотеза H_a про те, що послідовність – не випадкова. За результатами кожного тесту отримують висновок про прийняття або відхилення нульової гіпотези, ґрунтуючись на сформованій досліджуваним генератором послідовності. Кінцевим рішенням про те чи досліджувана послідовність є випадковою чи ні приймається за результатами сукупності усіх тестів [8].

Порядок тестування окремої двійкової послідовності S згідно з тестами NIST має такий вигляд [9]:

1. Висувається нульова гіпотеза H_0, тобто припущення про те, що дана двійкова послідовність S є випадковою.

2. За послідовністю S обчислюється статистика тесту c(S).

3. З використанням спеціальних функцій та статистики тесту обчислюється значення ймовірності $P = f(c(S))$, $P \in [0,1]$.

4. Значення ймовірності P порівнюється з рівнем значущості $\alpha, \alpha \in [0.001, 0.01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається, в іншому випадку приймається альтернативна гіпотеза.

Набір NIST складається з 15 статистичних тестів. Залежно від вхідних параметрів обчислюється 188 значень ймовірності P, які можна розглядати як результат роботи окремих тестів [10].

Таким чином, у результаті тестування двійкової послідовності формується вектор значень ймовірностей $P=\{P_1,P_2 \ldots P_{188}\}$. Аналіз складових P_i даного вектора дозволяє вказати на конкретні дефекти випадковості послідовності, що тестується.

За допомогою імітаційної моделі генератора ми змогли дослідити параметри різної кількості базових генераторів від двох до тридцяти.

Тест вважається пройденим, у тому випадку, коли імовірність проходження тесту P потрапить у межі від 0,98 до 1,00. Якщо ж імовірність P буде знаходитись нижче 0,98 вважається, що тест не пройдено. За отриманими результатами статистичного тестування будуємо статистичний портрет генераторів, який складається з матриці розміром m×q, де m – кількість двійкових послідовностей, які перевіряють, а q – кількість статистичних тестів, які використовуються для тестування кожної послідовності. Таким чином, статистичний портрет генератора – матриця розміром 1000×188, елементами якої є 188000 значень відповідних імовірностей.

Результати статистичних досліджень генераторів Голлмана подано на рис. 2-8. По вісі абсцис відкладено номер тесту NIST STS, по вісі ординат – імовірність проходження тесту.

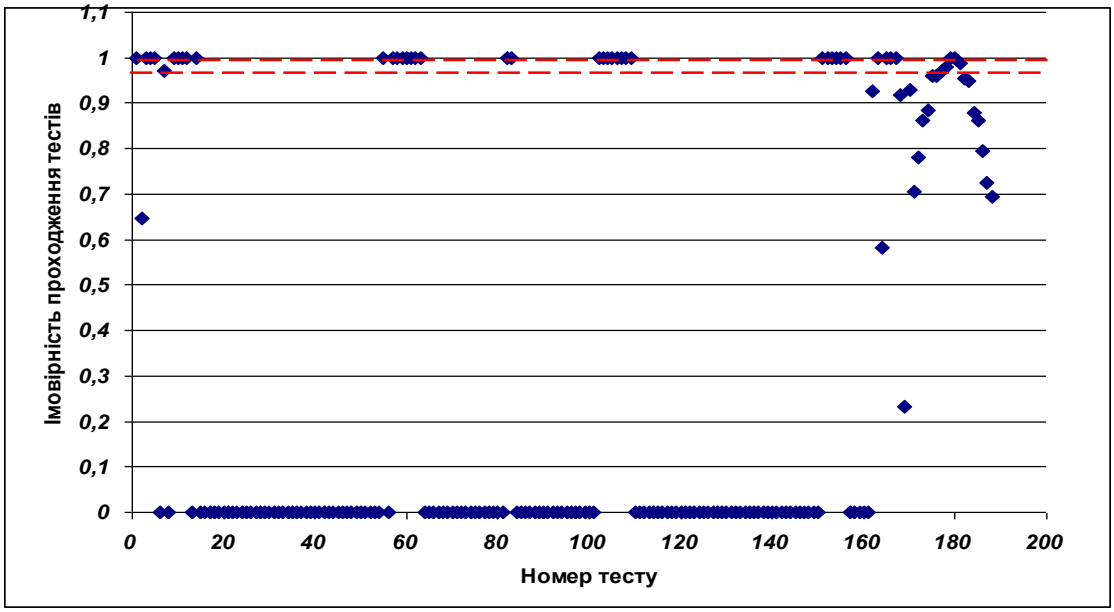

Рис. 2. Статистичний портрет генератора Голлманна з двома генераторами М-послідовності на основі твірного поліному $1 \oplus x^6 \oplus x^7$

Із статистичного портрета генератора видно, що більшість тестів знаходяться на смузі 0. А у виділений діапазон потрапляє лише декілька ітерацій тесту. З метою визначення оптимальних способів побудови генератора Голлманна змінювалась кількість базових генераторів М-послідовностей (рис.3-5).

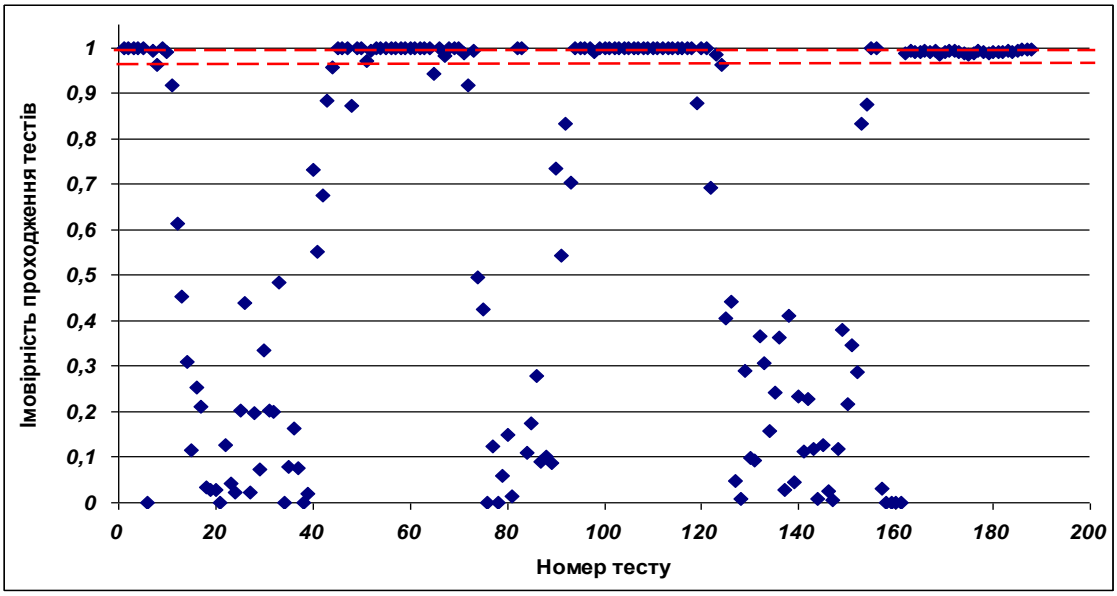

Рис. 3. Статистичний портрет генератора Голлманна з трьома генераторами М-послідовності на основі твірного поліному $1 \oplus x^6 \oplus x^7$

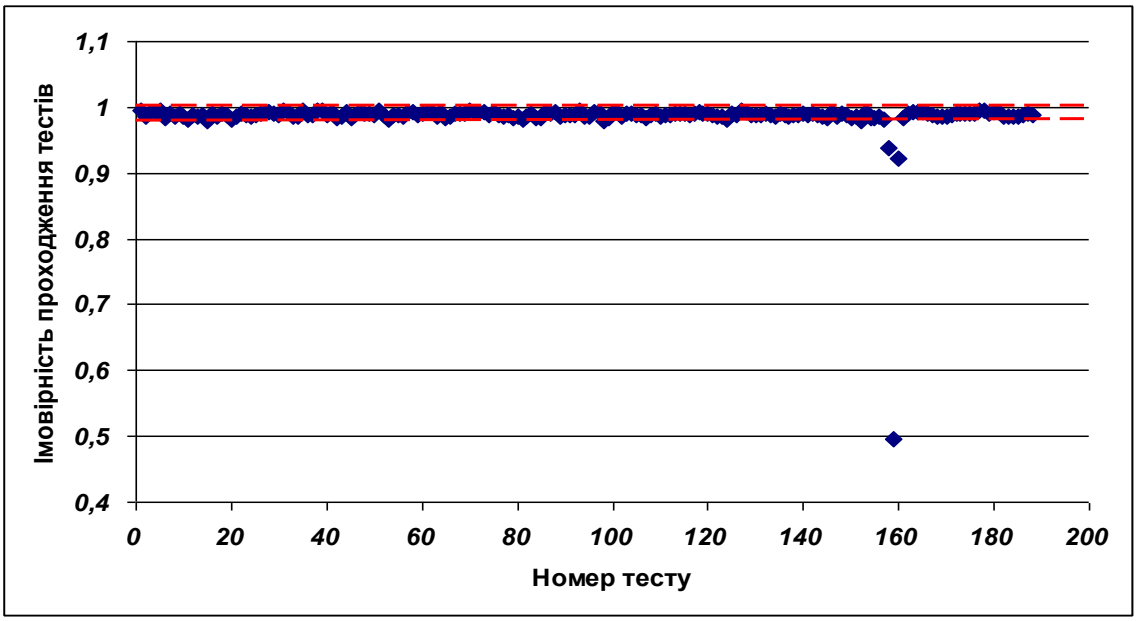

Рис. 4. Статистичний портрет генератора Голлманна з 5-ма генераторами М-послідовності на основі твірного поліному $1 \oplus x^6 \oplus x^7$

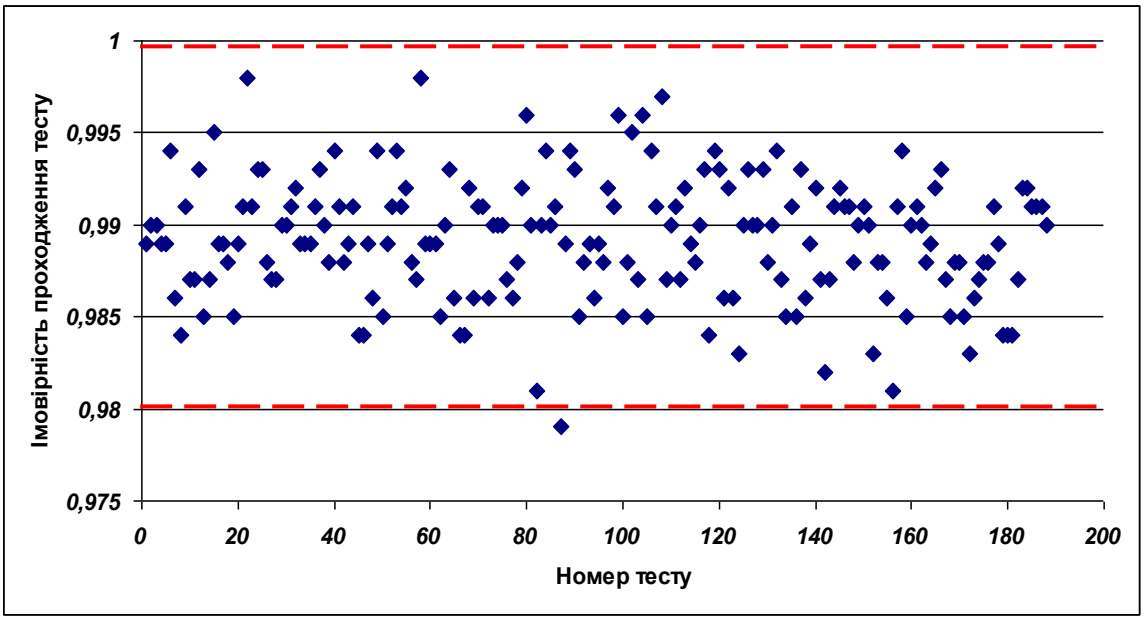

Рис. 5. Статистичний портрет генератора Голлманна з 7-ми генераторами М-послідовності на основі твірного поліному $1 \oplus x^6 \oplus x^7$

Як видно з наведених рисунків, із збільшенням кількості базових генераторів М-послідовностей якість генератора Голлманна покращується, оскільки кількість непройдених тестів зменшується.

Детальний звіт по оцінюванні за допомогою пакету статистичних тестів NIST вищезгаданих генераторів Голлманна, реалізованих на основі поліному 7-го степеня, наведено в таблиці 1.

Таблиця 1

Результати тестування генератора Голлманна на основі твірного поліному $1 \oplus x^6 \oplus x^7$

№	Статистичний тест	Кількість базових генераторів М - послідовності								
		2	*3*	*5*	*6*	*7*	*8*	*10*	*15*	*20*
1	Монобітний (частотний) тест	-	-	+	+	+	+	+	+	+
2	Частотний блоковий тест	-	-	+	+	+	+	+	+	+
3	Тест накопичених сум	-	-	+	+	+	+	+	+	+
4	Тест перевірки серій	-	-	+	+	+	+	+	+	+
5	Найдовшої серії одиниць	-	-	-	+	+	+	+	+	+
6	Перевірки рангу двійкових матриць	-	-	+	+	+	+	+	+	+
7	Тест на основі дискретного пертворення Фур'є	-	-	+	+	+	+	+	+	+
8	Тест на відповідність з шаблоном без перекриття	-	-	+	+	+	+	+	+	+
9	Тест на відповідність з шаблоном з перекриття	-	-	+	+	+	+	+	+	+
10	Універсальний тест Мауера	-	-	-	+	+	+	+	+	+
11	Тест на основі апроксимації ентропіїї	-	-	-	-	+	+	+	+	+
12	Тест серій	-	-	-	+	+	+	+	+	+
13	Тест лінійної складності	-	+	+	+	+	+	+	+	+
14	Тест випадкових блокувань	-	+	+	+	+	+	+	+	+
15	Тест випадкових блокувань 2	-	+	+	+	+	+	+	+	+

Аналогічні дослідження проводились над генераторами Голлманна реалізованими на основі поліномів інших степенів. Зокрема для поліномів 17-го степеня отримані наступні оцінки (рис.6-8).

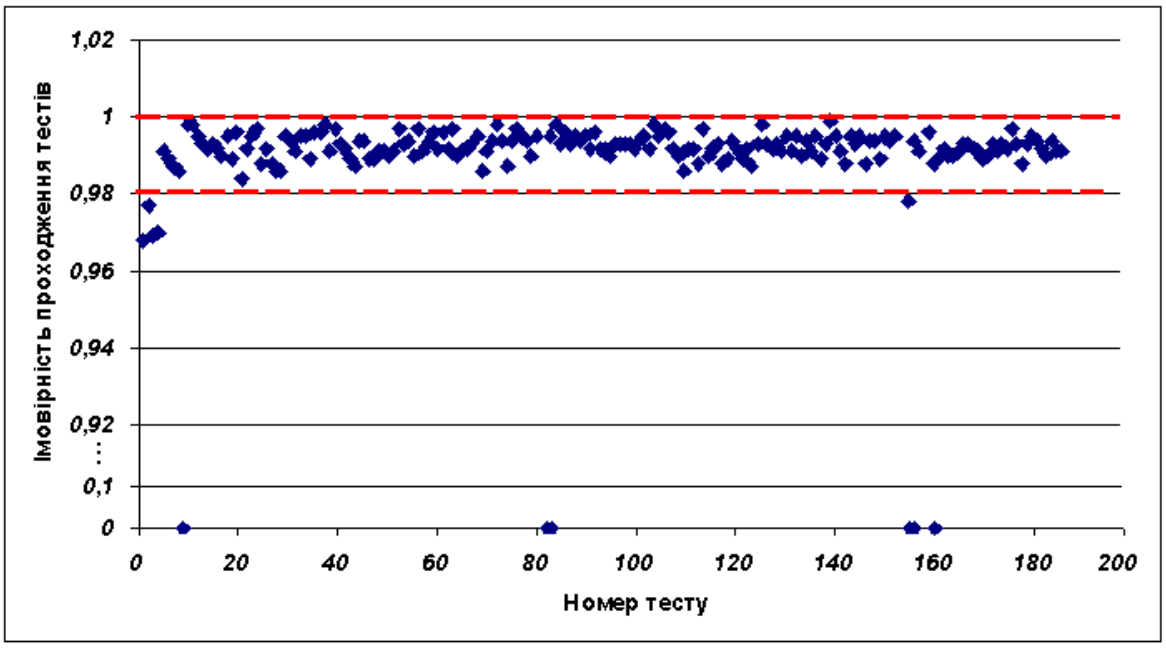

Рис. 6. Статистичний портрет генератора Голлманна з двома генераторами М-послідовності на основі твірного поліному $1 \oplus x^{12} \oplus x^{17}$

З наведеного графіку видно, що даний генератор не пройшов лише 7 тестів, що в порівнянні з аналогічним генератором Голлманна реалізованим на твірному поліномі $1 \oplus x^6 \oplus x^7$ є значно кращим результатом.

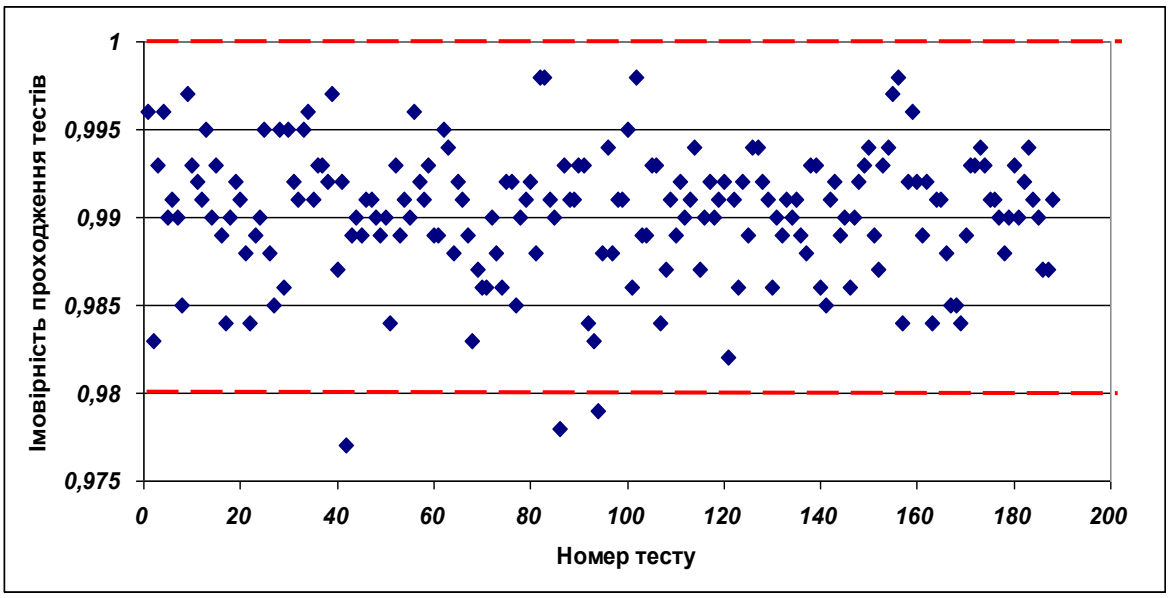

Рис. 7. Статистичний портрет генератора Голлманна з трьома генераторами М-послідовності на основі твірного поліному $1 \oplus x^{12} \oplus x^{17}$

Як видно з рисунку 7, отримані результати значно кращі попередніх, тільки три значення менші 0,98, отже збільшення кількості генераторів М-послідовності значно впливає на криптостійкість генератора. Це підтверджує наступний крок – вибір 5 генераторів.

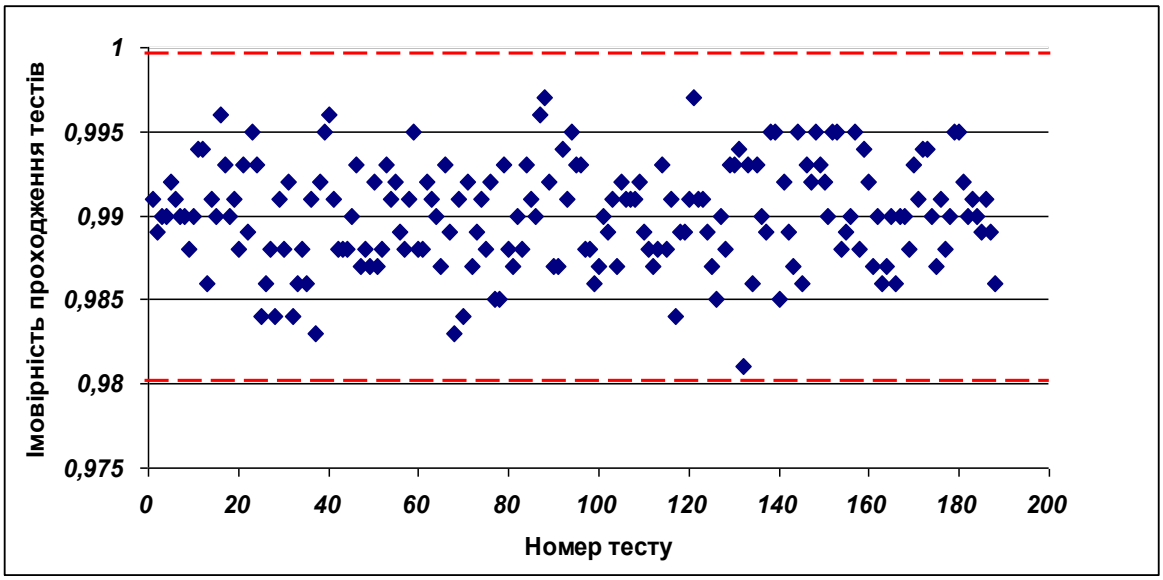

Рис. 8. Статистичний портрет генератора Голлманна з 5-ма генераторами М-послідовності на основі твірного поліному $1 \oplus x^{12} \oplus x^{17}$

Як бачимо з рисунку 8, 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 криптографічну стійкість.

Детальний звіт по оцінюванні за допомогою пакету статистичних тестів NIST вищезгаданих генераторів Голлманна, реалізованих на основі поліному 17-го степеня, наведено в таблиці 2.

Таблиця. 2

Результати тестування генератора Голлманна на основі твірного поліному $1 \oplus x^{12} \oplus x^{17}$

№	Статистичний тест	Кількість базових генераторів М - послідовності				
		2	*3*	*4*	*5*	*10*
1	Монобітний (частотний) тест	-	+	+	+	+
2	Частотний блоковий тест	-	+	+	+	+
3	Тест накопичених сум	-	+	+	+	+
4	Тест перевірки серій	-	+	+	+	+
5	Найдовшої серії одиниць	+	+	+	+	+
6	Перевірки рангу двійкових матриць	+	+	+	+	+
7	Тест на основі дискретного пертворення Фур'є	+	+	+	+	+
8	Тест на відповідність з шаблоном без перекриття	-	-	+	+	+
9	Тест на відповідність з шаблоном з перекриття	-	+	+	+	+
10	Універсальний тест Мауера	+	+	+	+	+
11	Тест на основі апроксимації ентропіїї	+	+	+	+	+
12	Тест серій	-	+	+	+	+
13	Тест лінійної складності	+	+	+	+	+
14	Тест випадкових блокувань	+	+	+	+	+
15	Тест випадкових блокувань 2	+	+	+	+	+

На рисунку 9 графічно показано середнє значення імовірності проходження тестів NIST STS досліджуваних генераторів Голлманна з різною кількістю базових генераторів М-послідовності і твірними поліномами $1 \oplus x^{6} \oplus x^{7}$ та $1 \oplus x^{12} \oplus x^{17}$.

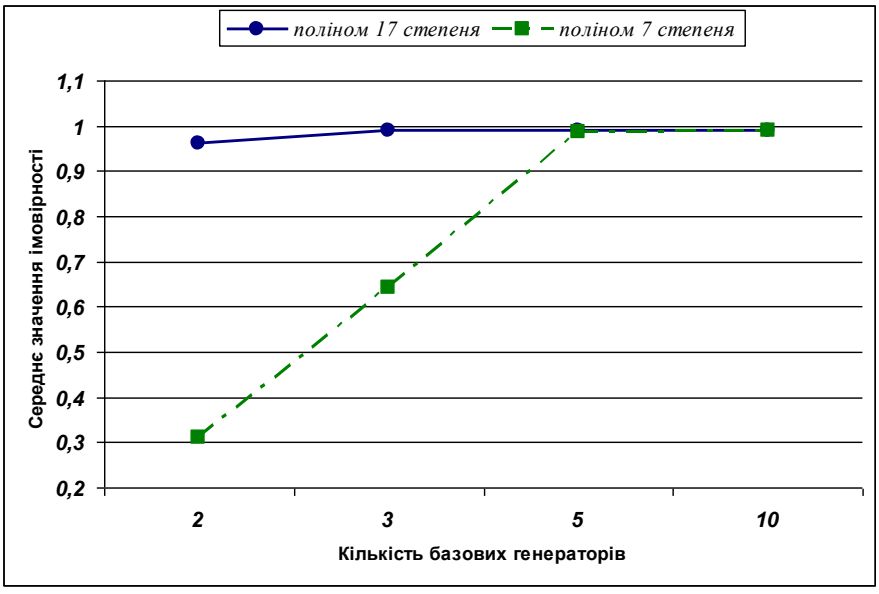

Рис. 9. Порівняння середнього значення імовірності проходження тестів NIST різними генераторами Голлманна

Висновки

Збільшення кількості базових генераторів М – послідовності і збільшення степенів їх поліномів приводить до підвищення якості генератора Голлманна. При цьому для зафіксованих значень цих кількостей генератор Голлманна проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики і криптостійкість.

Вибір конкретних параметрів генератора Голлманна повинен визначатись з заданими рівнями криптостійкостями і статистичними характеристиками, заданою швидкодією і оптимальним об’ємом обладнання, що може бути предметом подальших досліджень.

Література

1. Жельников В. Криптография от папируса до комп’ютера / В. Жельников – М.: ABF, 1996. – 254с.
2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ – ОБРАЗ, 2001. – 368 с.
3. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / Иванов М.А., Чугунков И.В. – М.: КУДИЦ – ОБРАЗ, 2003. – 240 с.
4. Гарасимчук О.І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / О.І. Гарасимчук, В.М. Максимович // “Захист інформації”. – м. Київ, 2002, 7 стор., 1 іл.
5. Гарасимчук О. І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей / О.І. Гарасимчук, В.М. Максимович // Вісник НУ “Львівська політехніка”. “Комп'ютерні науки та інформаційні технології”, – 2004. – №521 – С. 17-23.
6. Rock A. Pseudorandom Number Generators for Criptographic Applications / A. Rock. – Salzbuburg, 2005. – p. 57–65.
7. Вильданов Р.Р. Тесты псевдослучайных последовательностей и реализующее их программное средство / Вильданов Р.Р., Мещеряков Р.В., Бондарчук С.С. // журнал "Доклады Томского государственного университета систем управления и радиоэлектроники" № 1 (25), часть 2, – 2012 г. – 108 с.
8. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf
9. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Вид-во «Форт», 2012. – 880 с.
10. Статистические тесты NIST. [Електронний ресурс]. Режим доступу: http://ru.wikipedia.org/wiki/Статестичиские_тесты_NIST