Дослідження генератора Голлманна за допомогою статистичних тестів NIST

Юрій Костів[1], Володимир Максимович[1], Олег Гарасимчук[2], Марія Мандрона[1]

1. Кафедра безпеки інформаційних технологій, Національний університет "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 12, E-mail: yura.kostiv@gmail.com

2. Кафедра захисту інформації, Національний університет "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 12, E-mail: garasymchuk@ukr.net

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.

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

I. Вступ

На даний час розроблена велика кількість різноманітних методів та принципів генерування псевдовипадкових послідовностей, кожний з яких має свої переваги та недоліки [1-5]. Серед таких методів варто звернути увагу на генератор Голлманна. Зважаючи на те, що даний тип генераторів є недостатньо досліджений, то виникає задача, що полягає у покращенні характеристик генератора Голлманна з метою отримання на його виході послідовностей, що прямо чи опосередковано можна було б застосовувати при вирішенні задач захисту інформації.

Для того щоб робити висновок про можливість застосування того чи іншого генератора псевдовипадкової послідовності (ГПВП) для вирішення конкретних задач потрібно виконати оцінювання його якості та надійності. Тестування генераторів, особливо тих, що використовуються в криптографічних додатках є актуальною теоретичною та практичною задачею. На сьогоднішній день для тестування псевдовипадкових послідовностей розроблено кілька програмних продуктів, що містять комплекси тестів для перевірки різних статистичних властивостей, найвідомішим серед яких є набір статистичних тестів NIST [6,7].

II. Мета роботи

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

III. Генератор Голлманна та результати його досліджень

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

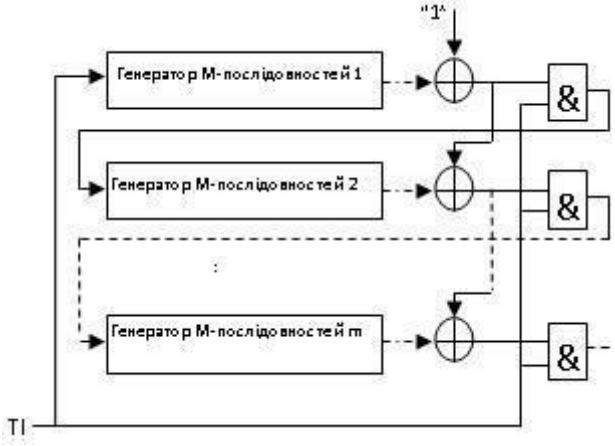

Рис.1. Генератор Голлманна

Для дослідження та оцінки якості генераторів Голлманна змінювалась розрядність базових генераторів М-послідовностей та кількість таких генераторів. Оцінювання якості виконувалось за допомогою набору статистичних тестів NIST. Результати такого оцінювання генератора Голлманна, на даний час, в літературі відсутні. Нами була розроблена імітаційна модель генератора на мові Delphi, яка дозволяє змінювати згадані вище параметри.

Базовим принципом тестування за допомогою статистичних тестів NIST є перевірка певної нульової гіпотези H0 про те, що послідовність, яка перевіряється є випадковою. З цією нульовою гіпотезою пов'язана альтернативна гіпотеза На 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 [6].

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.

Із збільшенням кількості базових генераторів М-послідовностей якість генератора Голлманна покращується, оскільки кількість непройдених тестів зменшується. Наприклад один з найкращих результатів для поліному 7-го степеня:

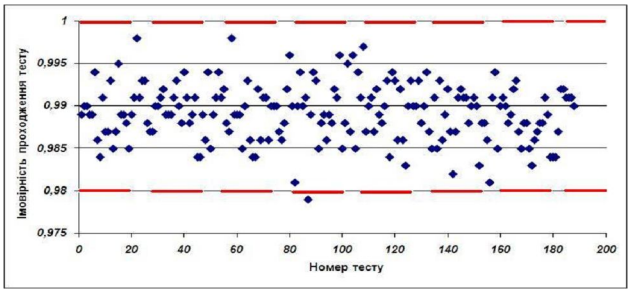

Рис. 2. Статистичний портрет генератора Голлманна з 7-ми генераторами М-послідовності на основі твірного поліному $1 \oplus \chi^6 \oplus \chi^7$

Детальний звіт наведено в таблиці 1.

ТАБЛИЦЯ 1

РЕЗУЛЬТАТИ ТЕСТУВАННЯ ГЕНЕРАТОРА ГОЛЛМАННА НА ОСНОВІ ТВІРНОГО ПОЛІНОМУ $1 \oplus \chi^6 \oplus \chi^7$

№	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 ентропії	-	-	-	-	+	+	+	+	+
12	Тест серій	-	-	-	+	+	+	+	+	+
13	Тест лінійної складності	-	+	+	+	+	+	+	+	+
14	Тест випадкових блокувань	-	+	+	+	+	+	+	+	+
15	Тест випадкових блокувань 2		+	+	+	+	+	+	+	+

Такі ж дослідження проводились над генераторами Голлманна реалізованими на основі поліномів інших степенів, зокрема для поліномів 17-го степеня. Результати були аналогічними – вже починаючи з 5 базових генераторів були пройдені всі тести.

На рисунку 2 графічно показано середнє значення імовірності проходження тестів NIST STS досліджуваних генераторів Голлманна з різною кількістю базових генераторів М-послідовності і твірними поліномами $1 \oplus \chi^6 \oplus \chi^7$ та $1 \oplus \chi^{12} \oplus \chi^{17}$.

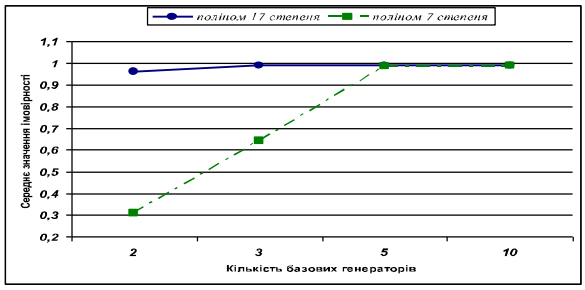

Рис. 3. Порівняння середнього значення імовірності проходження тестів NIST різними генераторами Голлманна

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] Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ – ОБРАЗ, 2001. – 368 с.

[2] Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / Иванов М.А., Чугунков И.В. – М.: КУДИЦ – ОБРАЗ, 2003. – 240 с.

[3] 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.

[4] 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.

[5] Rock A. Pseudorandom Number Generators for Criptographic Applications / A. Rock. – Salzbuburg, 2005. – p. 57–65.

[6] 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.

[7] Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Вид-во «Форт», 2012. – 880 с.