Способи покращення параметрів модифікованого генератора Голлманна

Володимир Максимович, Юрій Костів

Кафедра захисту інформації, Національний університет «Львівська політехніка», УКРАЇНА, м.Львів, вул. С.Бандери, 12, E-mail: Yura.Kostiv@gmail.com

Abstract. Research of the modified generator of Gollmanna. Increase period repetition of pseudorandom numbers generators (PRNG). Research was conducted with the help of the created simulation model.

Ключові слова – generator, pseudorendom numbers, M-sequences, simulation model, generator of Gollmanna.

Послідовність називається псевдовипадковою, якщо вона виглядає, як безсистемна і випадкова, хоча насправді вона створювалась з допомогою детермінованого процесу, відомого під назвою генератора псевдовипадкових чисел (ГПЧ) [1].

ГПЧ – фундаментальний стандартний блок для зміцнення і забезпечення конфіденційності зв'язків радіоелектронними засобами. Вони основний елемент криптографії, цифрового підпису, протоколів безпеки (надійності) і іншого забезпечення надійності при зв'язку через комп'ютер.

Криптографічні ГПЧ генерують псевдовипадкові числа, які використовуються в криптографічних застосуваннях, наприклад, для генерації ключів. [2] Для застосування в криптографічних системах ГПЧ повинні відповідати наступним вимогам:

- послідовність, яка генерується повинна мати великий період;
- послідовність, яка генерується не повинна мати схованих періодичностей;
- послідовність, яка генерується повинна мати рівномірний спектр.

Генератор Голлманна, що відноситься до потокових генераторів псевдовипадкових чисел дозволяє за рахунок нескладних схемотехнічних рішень істотно збільшити період повторення псевдовипадкової імпульсної послідовності [3].

Одним з можливих видів генераторів, які працюють на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (Linear Feedback Shift Register) [4, 5, 6], є генератор Д. Голлманна. В його роботі використовується принцип stop – and – go (структурна схема показана на рис.1). Кожен генератор LFSR (i) управляє синхронізацією двох наступних LFSR (i+1) і LFSR (i+2). Вихід останнього LFSR є виходом генератора. Якщо розрядність кожного LFSR рівна N, лінійна складність системи з m LFSR рівна

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

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

Метою дослідження було з'ясування впливу параметрів складових частин генератора на характеристики його вихідного сигналу. Враховуючи велику кількість можливих варіантів побудови генератора Голлманна, дослідження проводились із зміною наступних чинників:

- кількості регістрів зсуву з лінійними зворотними зв'язками (LFSR);
- структурних схем самих LFSR;
- введенням додаткових зв'язків між окремими LFSR, що дозволяє віднести досліджувані генератори до модифікованих.

Дослідження проводились з допомогою імітаційної моделі, створеної в середовищі Delphi. Було створено кілька програм:

- програма для визначення поточних значень вихідного сигналу;
- програма для визначення статистичних характеристик, що дозволяє досліджувати кількості вихідних імпульсів на певних інтервалах значень тактових сигналів;
- програма для перевірки рівномірності розподілу символів 0 і 1 у вихідному сигналі;

Структурна схема генератора наведена на рис.1

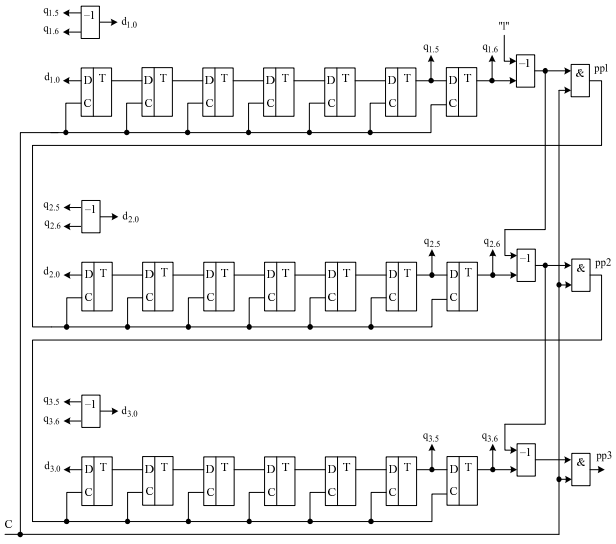


Рис. 1. Структурна схема генератора Голлманна

В роботі досліджувались не тільки параметри вихідного сигналу pp3 (вихід LFSR3), але й параметри проміжних імпульсних потоків pp1 (на виході LFSR1) і pp2 (на виході LFSR2). Регістри LFSR1, LFSR2, LFSR3 побудовані у відповідності до логічних рівнянь (2.1)-(2.3) відповідно:

$$q_{1.0}(i+1) = q_{1.5}(i) \oplus q_{1.6}(i) \qquad q_{2.0}(i+1) = q_{2.5}(i) \oplus q_{2.6}(i) \qquad q_{3.0}(i+1) = q_{3.5}(i) \oplus q_{3.6}(i)$$

$$q_{1.1}(i+1) = q_{1.0}(i) \qquad q_{2.1}(i+1) = q_{2.0}(i) \qquad q_{3.1}(i+1) = q_{3.0}(i)$$

$$q_{1.2}(i+1) = q_{1.1}(i) \qquad q_{2.2}(i+1) = q_{2.1}(i) \qquad q_{3.2}(i+1) = q_{3.1}(i)$$

$$q_{1.3}(i+1) = q_{1.2}(i) \qquad q_{2.3}(i+1) = q_{2.2}(i) \qquad q_{3.3}(i+1) = q_{3.2}(i)$$

$$q_{1.4}(i+1) = q_{1.3}(i) \qquad q_{2.4}(i+1) = q_{2.3}(i) \qquad q_{3.4}(i+1) = q_{3.3}(i)$$

$$q_{1.5}(i+1) = q_{1.4}(i) \qquad q_{2.5}(i+1) = q_{2.4}(i) \qquad q_{3.5}(i+1) = q_{3.4}(i)$$

$$q_{1.6}(i+1) = q_{1.5}(i) \qquad q_{2.6}(i+1) = q_{2.5}(i) \qquad q_{3.6}(i+1) = q_{3.5}(i)$$

(2.1) (2.2) (2.3)

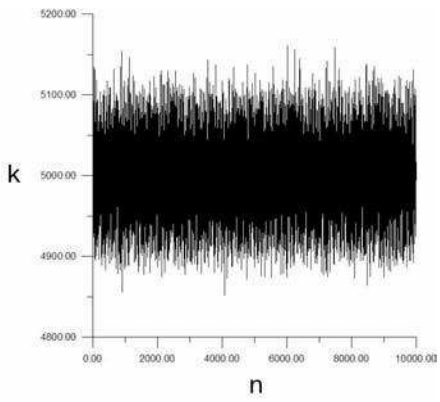
Для досліджень використовувались базові генератори М-послідовностей різної розрядності. А саме,

побудова генератора Голлманна проводилась на основі генераторів М-послідовностей розрядності N=7, N=17 для примітивних поліномів $\Phi(x) = 1 \oplus x^6 \oplus x^7$ та $\Phi(x) = 1 \oplus x^6 \oplus x^{17}$.

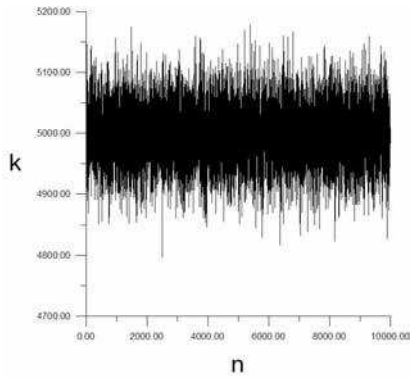
Відомо, що якщо генератор М-послідовностей побудований на основі твірного поліному відповідного степеня, тоді він має максимальний період повторення чисел, що генеруються .

Завдяки цьому можна отримати псевдовипадкові послідовності з періодом повторення 2^N-1 для кожного полінома, що є достатньо для забезпечення широкого діапазону вихідних частот [7, 8].

На рис. 2 (а-б) наведені графіки залежностей $k(n)$, які визначають кількості імпульсів на виході LFSR3, що відповідає і тактовим сигналам, де $n = 1,2,3,...$ – номер чергового інтервалу.



а) при примітивному поліномі $\Phi(x) = 1 \oplus x^6 \oplus x^7$



б) при примітивному поліномі $\Phi(x) = 1 \oplus x^6 \oplus x^{17}$

Рис. 2. Статистичні характеристики сигналів генератора Голлманна

Дослідження проводились при змінній кількості розрядів усіх LFSR, отже, їх задачею було не лише виявлення тенденцій зміни параметрів вихідного сигналу генератора в залежності від параметрів його структурної схеми, але і дослідження якості псевдовипадкової послідовності при різних примітивних поліномах, та кількості генераторів LFSR.

Таким чином, створена імітаційна модель дозволяє оперативно досліджувати різні варіанти генераторів Голлманна. Отримані результати дозволяють вибрати способи покращення його характеристик.

1. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ – ОБРАЗ, 2003 – 240 с. – (СКБ – специалисту по компьютерной безопасности).
2. Кнут Д. Искусство программирования для ЭВМ: В 3-х т. Получисленные алгоритмы. Пер. с англ. – М.: Мир, 1977. – Т.2. – 724с.
3. Белов А.Г., Галкин В.Я. Ассимптотическая эффективность совместного оценивания параметров сложнопуассоновского распределения // Численные методы решения обратных задач математической физики. М.: Изд-во Моск. Ун-та, 1988, с. 46-57.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. И доп. – М.: Радио и связь, 2001. – 376 с.: ил.
5. Гарасимчук О.І., Максимович В.М., Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості // Захист інформації, м.Київ, №3, 2003. – с. 29-36.
6. Гарасимчук О.І., Дудикевич В.Б., Максимович В.М. Кількісне оцінювання генератора пуассонівської імпульсної послідовності побудованого на основі конгруентного генератора // Вісник Східно-Українського національного університету ім. Даля. №9 (103). Науковий журнал. Частина І. Луганськ, 2006 – с.53-56.
7. Гарасимчук О.І., Дудикевич В.Б., Максимович В.М. Кількісне оцінювання генератора пуассонівської імпульсної послідовності на основі генератора М-послідовності // Вісник ДУІКТ - №4, том 4, 2006. с.251-258.
8. Гарасимчук О.І., Максимович В.М. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей // Вісник НУ “Львівська політехніка” - “Комп’ютерна інженерія та інформаційні технології”. - 2004 №521. - С. 17-23.