Дослідження генератора псевдовипадкових бітових послідовностей на основі LFSR при різних степенях формуючої матриці

Микола Шевчук[1], Володимир Максимович[2], Марія Мандрона[3]

1. Кафедра безпеки інформаційних технологій, Національний університет "Львівська політехніка", УКРАЇНА, м.Львів, вул.С.Бандери, 12, E-mail: shevchuk.mykola93@gmail.com

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

3. Кафедра управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, УКРАЇНА, м. Львів, вул. Клепарівська,35, E-mail: mandrona27@gmail.com

The article presents the results of LFSR (linear feedback shift register) generator estimation with a different degrees of output polynomials, with a different initial states and with a different degrees of input matrix, 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 pseudorandom sequence.

Ключові слова – генератор псевдовипадкових послідовностей, захист інформації, псевдовипадкові числа, статистичні характеристики.

Вступ

Генератори псевдовипадкових чисел (ГПЧ) і псевдовипадкових бітових послідовностей (ГПВБП) часто зустрічається в багатьох областях вимірювальної техніки, системах захисту інформації, при моделюванні різних систем та процесів. При цьому вимоги до їх статистичних характеристик відрізняються в залежності від області їхнього застосування. Генерування псевдовипадкових послідовностей і перевірка на випадковість згенерованої послідовності є одними з найважливіших проблем сучасної криптології. В сучасних криптосистемах генератори псевдовипадкових послідовностей використовуються для створення ключової інформації і забезпечення параметрів цих систем.

Рис. 1. Спрощена структурна схема генератора на основі LFSR

Метою роботи є використання статистичних тестів національного інституту стандартів і технологій (NIST) США для тестування генераторів псевдовипадкових бітових послідовностей на основі лінійних регістрів зсуву(LFSR) при різних початкових станах, при різних степенях формуючої матриці та при різних поліномах. Спрощена структурна схема генератора на основі LFSR наведена на рис. 1.

Генератори псевдовипадкових бітових послідовностей на основі LFSR

Відомо, що окремо взяті генератори псевдовипадкових бітових послідовностей (ГПВБП) на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR не відносяться до криптостійких [1,2]. Незважаючи на це, вони часто використовуються як структурні елементи більш складних пристроїв, зокрема при реалізації потокових шифрів (наприклад, алгоритми – A3, A5, A8, PIKE, SEAL, RC4). Основною їх перевагою є велика швидкодія і простота при апаратній реалізації.

Статистичні характеристики ГПВБП на основі LFSR розглядались в багатьох роботах [1, 2]. Однак, залишаються не повністю визначена мінімальна кількість структурних елементів LFSR, і пристроїв на їх основі, при яких досягається статистична безпека, тобто статистичні характеристики вихідної бітової послідовності є задовільними;

Проведені в даній роботі дослідження направлені на часткове вирішення вказаних задач. При цьому вважаємо, що статистичні характеристики ГПВБП є задовільними, якщо вихідна бітова послідовність генератора проходить усі тести NIST [5], а при комплексному порівнянні генераторів на різних базах, окрім їх статистичних характеристик необхідно також розглянути: періоди повторення вихідної послідовності, складність побудови (технологічність) при реалізації на програмованих логічних схемах (ПЛІС) і максимально можливу довжину криптографічного ключа, однак в цій роботі акцентовано увагу на дослідженні статистичних характеристик ГПВБП за різних умов.

Варто підкреслити, що криптостійкість таких генераторів, без криптоаналізу, не є гарантованою. Статистична безпека, як відомо, є для цього необхідною, але не достатньою умовою [2].

Варіанти побудови ГПВБП на основі LFSR, необхідно розглядати, виходячи з рівняння його функціонування

$$Q(t+1) = T^r Q(t), \qquad (1)$$

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

$$T_1 = \begin{vmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ 1 & 0 & & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ & & & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix} \text{ або } T_2 = \begin{vmatrix} 0 & \dots & 0 & 0 & a_n \\ 1 & \dots & 0 & 0 & a_{n-1} \\ & & & & \\ 0 & \dots & 1 & 0 & a_2 \\ 0 & \dots & 0 & 1 & a_1 \end{vmatrix}; \qquad (2)$$

n– степінь многочлена

$$F(x) = \sum_{i=0}^{n} a_i x^i, \quad a_n = a_0 = 1, \quad a_j \in \{0,1\}, \quad j = \overline{1,(n-1)}; \qquad (3)$$

r – степінь формуючої квадратної матриці [1].

Отже, LFSR різняться:

– степенем і видом твірного поліному [3], що задають кількість розрядів регістра зсуву і впливають на форму зворотних зв'язків;

– виглядом (Т1 чи Т2) і степенем r формуючої квадратної матриці, що задають спосіб формування зворотних зв'язків і формують їх остаточну конфігурацію.

Нами, з допомогою імітаційного моделювання і тестів NIST, були досліджені характеристики генератора при різних твірних поліномах, різних степенях формуючої квадратної матриці, та при різних початкових станах.

Таблиця 1

Результати тестів NIST ГПБП при різних твірних поліномах та різних початкових станах і степенях

Вхідний поліном	$x^{100}+x^{37}+1$		
Степінь формуючої квадратної матриці	1	5	10
Початковий стан 1	-	-	-
Початковий стан 2	-	-	-
Початковий стан 3	-	-	-
Вхідний поліном	$x^{150}+x^{53}+1$		
Початковий стан 1	-	-	-
Початковий стан 2	-	-	-
Початковий стан 3	-	-	-
Вхідний поліном	$x^{201}+x^{14}+1$		
Початковий стан 1	-	-	-
Початковий стан 2	-	-	-
Початковий стан 3	-	-	-
	$x^{270}+x^{133}+1$		
Початковий стан 1	-	-	-
Початковий стан 2	-	+	+
Початковий стан 3	-	+	+
	$x^{322}+x^{67}+1$		
Початковий стан 1	-	-	-
Початковий стан 2	-	+	+
Початковий стан 3	-	+	+
	$x^{378}+x^{43}+1$		
Початковий стан 1	-	-	-
Початковий стан 2	-	+	+
Початковий стан 3	-	+	+

- Початковий стан 1 – перший біт «1» решта бітів «0».
- Початковий стан 2 – останній біт «0» решта бітів «1».
- Початковий стан 3 – половина бітів «1» інша половина «0».

Аналіз дослідження

Аналіз, за допомогою тестів NIST, наведеного генератора показав, що його статистичні характеристики не відповідають вимогам випадковості при степені формуючої квадратної матриці r рівній одиниці. Проте, якщо збільшити степінь матриці r, то псевдовипадкова послідовність згенерована цим ГПВБП проходить усі статистичні тести.

Починаючи з 270-и розрядного LFSR і при степені формуючої матриці r більший 5-и генератори псевдовипадкових послідовностей можна назвати статистично безпечними.

Висновок

Здійснене дослідження ГПВБП на основі LFSR показало, що навіть при великих значеннях степенів твірних поліномів генератори не є повністю статистично безпечними, однак змінивши степінь формуючої квадратної матриці r, можна досягнути статистичної безпеки. Таким чином, досліджувані генератори можуть бути використані як складові частини криптографічних систем.

Література

[1] Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванова, И.В. Чугунков. – М. : НИЯУ МИФИ, 2012. – 400 с.

[2] Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

[3] Мандрона М.Н. Исследование статистических характеристик модифицированных генераторов Фибоначчи / М.Н. Мандрона, В.Н. Максымовыч // Проблемы управления и информатики : межд. наук.-техн. журн. – 2014. – №6. – С. 28-36.

[4] Mandrona M.M. Examination of multi link generators of pseudorandom sequences built using R-blocks / M.M. Mandrona, Yu.M. Kostiv, V.M. Maksymovych, O.I. Harasymchuk // Sustainable development : International journal. – Varna : Euro-Expert Ltd. – 2014. – № 18. – Pp. 110-118.

[5] NIST SP 800-22. A Statistic Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application: [Електронний ресурс], April 2000. Режим доступу: http://csrc.nist.gov./publications/niatpubs//SP800-22rev1a.pdf.

Tempus

ENGENSEC
Educating the Next generation experts in Cyber Security

Міністерство освіти і науки України
Національна академія наук України
Міністерство науки та вищої освіти Республіки Польща
Національний університет "Львівська політехніка"
Інститут прикладних проблем механіки і математики ім. Я. С. Підстригача НАН України
Одеський національний політехнічний університет
Університет Бєльсько-Бяла (Польща)

ЗАХИСТ ІНФОРМАЦІЇ І БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

МАТЕРІАЛИ
VI МІЖНАРОДНОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

1–2 червня 2017 р.