УДК 004.421.5

С.О. Проскурін, О.М. Гапак, канд. пед. наук, доц.
Україна, Ужгород, ДВНЗ "Ужгородський національний університет", Україна

ВИЗНАЧЕННЯ ДОВЖИНИ ПЕРІОДУ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ LFSR ТА FCSR

S.O. Proskurin, O.M. Hapak, ph.D, Assoc.Prof

DETERMINATION PERIOD OF GENERATORS PSEUDORANDOM SEQUENCES BASIC ON LFSR AND FCSR

Генератори псевдовипадкових послідовностей (ГПВП) є важливими елементами будь-якої системи захисту, надійність якої в значній мірі визначається саме властивостями використовуваних генераторів. У криптографії псевдовипадкові послідовності (ПВП) використовуються для генерування ключів симетричних та асиметричних криптосистем; потокового шифрування; генерування електронного цифрового підпису тощо. Якісний ГПВП повинен створювати послідовність, яка за характеристиками наближається до випадкової. Під час проектування ГПВП необхідно враховувати ряд основних вимог: велика довжина періоду; висока продуктивність алгоритму; простота апаратної та програмної реалізації; ПВП не повинна бути передбачуваною та інші [1; 2].

Генератор псевдовипадкових послідовностей *LFSR.* Лінійний регістр зсуву зі зворотнім зв'язком (*LFSR*) – це пристрій, що складається з регістру зсуву, здатного запам'ятовувати двійкові послідовності кінцевої довжини та схеми, яка реалізовує додавання за модулем 2 (mod2). [3]

Рисунок 1. Генератор *LFSR*

Генератори псевдовипадкових послідовностей *FCSR*

Регістр зсуву зі зворотнім зв'язком та перенесенням (*FCSR)*, схожий на *LFSR*, в обох є регістр зсуву та функція зворотного зв'язку, різниця полягає у тому, що у *FCSR* є ще регістр перенесення. У порівнянні з *LFSR*, замість *mod 2* над усіма бітами відвідної послідовності, ці біти додаються один з одним і вмістом регістру перенесення.

Результат *mod 2* стає новим бітом, результат *div 2* стає новим вмістом регістру перенесення. [3]

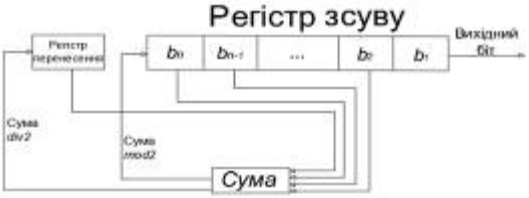

Рис. 2 – Генератор *FCSR*

Комбінації *LFSR, FCSR*:

- Генератор парності;
  Виходи генераторів *LFSR* та *FCSR* об'єднані функцією xor.
- Пороговий генератор;

Для даного генератора необхідно використовувати непарну кількість генераторів. Якщо більше половини вихідних бітів генераторів дорівнюють 1, то виходом генератора буде – 1, в іншому випадку – 0.

- Каскад Голлмана.

Каскад Голлманна складається із деякої послідовності генераторів *FCSR* та *LFSR*, тактування кожного з яких керується попереднім генератором. Якщо виходом *FCSR1* в момент часу t є 1, то тактується *LFSR*1, інакше повторюється попереднє значення *LFSR* - 1. Якщо *LFSR* - 1 в момент часу *t* є 1, то тактується *FCSR-2* і т.д. Вихід останнього генератора є виходом каскаду Голлманна.[3]

Визначення періоду послідовності

Період є однією з ключових характеристик якості генератора псевдовипадковою послідовності. Чим більший період, тим кращі криптографічними характеристики послідовності.

Наступні наші дослідження спрямовані на порядку розташування регістрів *FCSR* та *LFSR* із різними відвідними послідовностями в каскаді Голлманна. Для експериментів ми обрали: *FCSR* – 1 (1,2,3); *LFSR* – 1 (1,4); *FCSR* – 2 (1,2,3,4); *LFSR* – 2 (2,5); *FCSR* – 3 (1,2,4,5), із періодами: $T_1 = 12$, $T_2 = 15$, $T_3 = 28$, $T_4 = 31$, $T_5 = 52$. Результати дослідження подані у таблиці 1, де НСК– найменше спільне кратне вказаних чисел.

Таблиця 1 – Довжина періоду в залежності від порядку регістрів

№	Послідовність базових регістрів	Довжина періоду *T*
1	FCSR-1; LFSR1; FCSR-2; LFSR2; FCSR-3	338520 (2*НСК)
2	FCSR-1; LFSR2; FCSR-2; LFSR1; FCSR-3	338520 (2*НСК)
3	FCSR-1; LFSR1; FCSR-3; LFSR2; FCSR-2	338520 (2*НСК)
4	FCSR-1; LFSR2; FCSR-3; LFSR1; FCSR-2	135408 (0,8*НСК)
5	FCSR-2; LFSR1; FCSR-1; LFSR2; FCSR-3	507780 (3*НСК)
6	FCSR-2; LFSR2; FCSR-1; LFSR1; FCSR-3	507780 (3*НСК)
7	FCSR-2; LFSR1; FCSR-3; LFSR2; FCSR-1	169260 (НСК)
8	FCSR-2; LFSR2; FCSR-3; LFSR1; FCSR-1	338520 (2*НСК)
9	FCSR-3; LFSR1; FCSR-1; LFSR2; FCSR-2	507780 (3*НСК)
10	FCSR-3; LFSR2; FCSR-1; LFSR1; FCSR-2	507780 (3*НСК)
11	FCSR-3; LFSR1; FCSR-2; LFSR2; FCSR-1	169260 (НСК)
12	FCSR-3; LFSR2; FCSR-2; LFSR1; FCSR-1	507780 (3*НСК)
Генератор парності		169260 (НСК)
Пороговий генератор		169260 (НСК)

Із результатів таблиці 1 можна зробити висновок, що порядок розміщення регістрів значно впливає на його період. Базові компоненти потрібно розташувати в порядку спадання їх періодів.

Із результатів досліджень генераторів псевдовипадкових послідовностей на основі регістрів зсуву бачимо, що використання різних комбінацій FCSR та LFSR збільшують довжину періоду послідовності. Надалі необхідно провести статистичні оцінки якості таких генераторів.

Література

1. Гарасимчук О. І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / О. І. Гарасимчук, В. М. Максимович // Захист інформації. – К., 2002. – 7 с.

2. Харин Ю. С. Математические и компьютерные основы криптологии: учеб. пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. – Минск: Новое знание, 1999. – 319 с.

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