УДК 004.421.5

О.М. Гапак, Ужгород

ВИЗНАЧЕННЯ ДОВЖИНИ ПЕРІОДУ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ РЕГІСТРІВ ЗСУВУ ЗІ ЗВОРОТНІМ ЗВ'ЯЗКОМ ТА ПЕРЕНЕСЕННЯ

Abstract. The article under consideration is presented by the results of researches of pseudorandom sequences generator on the basis of Feedback with Carry Shift Register. It was defined the maximum length of the period, which provided various combinations of the given generators. The obtained results can effectively design algorithms for generating pseudorandom sequence with the maximum length of the period.

Вступ

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; 4].

Однією з основних характеристик є період ПВП – кількість псевдовипадкових чисел у послідовності, після якої вони починають повторюватись. Чим більший період, тим для довших відкритих текстів її можна застосовувати. Чим менший період, тим легше передбачувати числа в ній і зламувати ключі та шифри. Довжина періоду послідовності залежить від обраного алгоритму ГПВП.

Існує велика кількість різноманітних методів та принципів генерування ПВП. Одним із найпростіших у реалізації і найпоширеніших є ГПВП на основі регістрів зсуву з лінійним зворотнім зв'язком – LFSR (Linear Feedback Shift Register). Ці генератори знайшли широке використання у різних галузях науки і техніки [2; 3]. У сучасній літературі достатньо висвітлені дослідження даних генераторів, приведені оцінки їх якості. На відміну від LFSR, генератори на основі регістрів зсуву зі зворотнім зв'язком та перенесення – FCSR (Feedback with Carry Shift Register) є малодослідженими. Ідея використання FCSR є досить новою і вперше подана Енді Клаппером і Марком Горескі [8]. Один FCSR без підключення лінійного компоненту не доцільно використовувати у криптографії. У 2002 році Франсуа Арно, Террі

Бергер створили шифр, заснований на сумісному використанні FCSR та LFSR [6]. У 2005 році запропонували ідею сумісного використання FCSR і лінійного фільтру для створення шифру, що отримав назву F-FCSR [7]. Брюс Шнайер у праці [5] представив загальні ідеї побудови потокових шифрів на базі FCSR. Тому великий інтерес являє собою проведення оцінки якості ГПВП на основі FCSR, у тому числі, визначення їх основної характеристики – довжини періоду.

Метою даної роботи є визначення довжини періоду ГПВП на основі FCSR.

Генератори псевдовипадкових послідовностей побудовані на основі FCSR

FCSR схожий на LFSR, в обох є регістр зсуву та функція зворотного зв'язку, різниця полягає у тому, що у FCSR є також регістр перенесення. Існують два варіанти реалізації FCSR: конфігурація Галуа та Фібоначчі. Ми розглядатимемо конфігурацію Фібоначчі. У порівнянні з LFSR, замість *xor* 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 (рис.1).

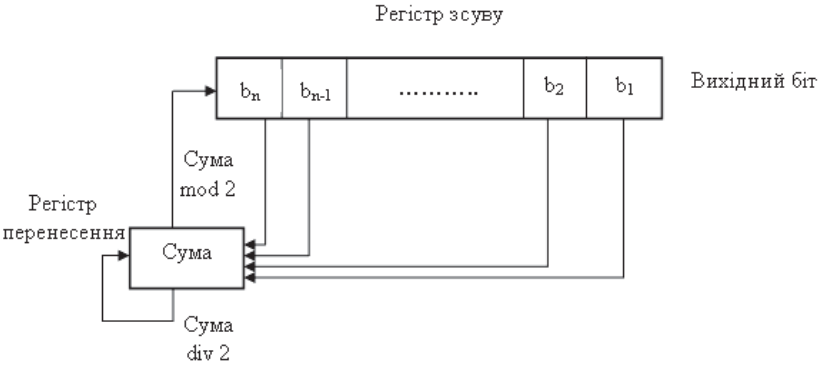

Рис. 1. FCSR

Існує початкова затримка, перш ніж FCSR перейде у циклічний режим. Початковий стан FCSR відповідає ключу потокового шифру. Будь-який початковий стан приводить до однієї із чотирьох ситуацій. По-перше, він може бути частиною максимального періоду. По-друге, він може перейти у послідовність максимального періоду після початкової затримки. По-третє, після початкової затримки може утворитися нескінчена послідовність нулів. По-четверте, після початкової затримки може утворитися нескінчена послідовність одиниць. Для визначення, чим закінчиться конкретний початковий стан, існує математична формула, але набагато простіше

визначити це дослідним шляхом: згенерувати *n* бітів, де *n* – довжина FCSR і зробити відповідні висновки [5].

Регістр перенесення – не біт, а число, розмір якого повинен бути не менше $\log_2 t$, де *t* – кількість розгалужень у відвідній послідовності. Якщо є два розгалуження, то регістр перенесення однобітний; якщо три, чотири розгалуження, то регістр перенесення двобітний і т.д.

Максимальний період FCSR дорівнює *q*-1, де *q* – ціле число зв'язку. Це число задає розгалуження і визначається за формулою $q = 2q_1 + 2^2 q_2 + ... + 2^n q_n - 1$, де q_i відраховується зліва направо. Наприклад, для 4-бітного регістру $b_4 b_3 b_2 b_1$, відраховуємо $q_1 q_2 q_3 q_4$. Крім того, *q* – просте число, для якого 2 є примітивним коренем. У праці Б. Шнайера [5] перераховано всі цілі числа зв'язку, менші за 1000, для FCSR з максимальним періодом та наведено перелік відвідних послідовностей із чотирьох розгалужень, які дають максимальний період для 32-бітних, 64-бітних, 128-бітних FCSR. Для створення послідовності з максимальним періодом можна використовувати будь-яку із цих послідовностей. Якщо відвідна послідовність задана у вигляді (*a*,*b*,*c*,*d*), то $q = 2^a + 2^b + 2^c + 2^d - 1$.

Для прикладу побудуємо ПВП на основі FCSR з числом зв'язку *q*=19. Для того, щоб визначити відвідну послідовність, необхідно розрахувати бінарний склад числа *q*+1.

$$20 = 2^4 + 2^2 = 2 \cdot 0 + 2^2 \cdot 1 + 2^3 \cdot 0 + 2^4 \cdot 1.$$

Відвідна послідовність (4, 2), це означає, що у розгалуженні будуть приймати участь b_3 та b_1 біти регістру зсуву. Так як кількість розгалужень дорівнює 2, то для регістру перенесення необхідно лише один біт. Задамо початковий стан регістру зсуву – (1010) та регістру перенесення – 0. Отримаємо наступну послідовність бітів: 01010011110101100001…., довжина періоду якої становить *q*–1=18.

Для *n*-бітного LFSR максимальна довжина періоду становить 2^n–1, що суттєво менше довжини періоду *n*-бітного FCSR.

Наприклад, для 32-розрядного LFSR із твірним поліномом $x^{32} + x^7 + x^5 + x^3 + x^2 + x^1 + 1$, або (32,7,5,3,2,1,0), довжина періоду становить $2^{32} - 1 = 4294967295$. Для відвідної послідовності (32,31,30,2) 32-розрядного FCSR довжина періоду дорівнює $2^{32} + 2^{31} + 2^{30} + 2^2 - 1 = 7516192771$.

Основний підхід до проектування ГПВП на основі FCSR аналогічний як і для LFSR, а саме, використовуються декілька регістрів з різними довжинами, які об'єднані лінійним чи нелінійним способом [5].

Розглянемо деякі види таких генераторів:

1. Генератор парності. Регістри FCSR об'єднані функцією *xor* (рис.2).

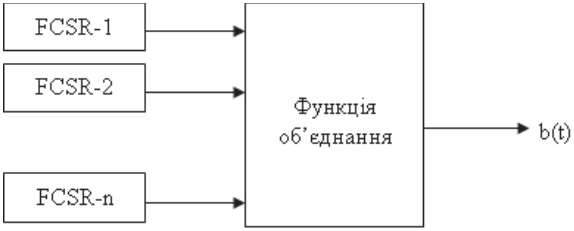

Рис. 2. Генератор парності

Дослідивши ПВП, яка побудована за даним принципом, можемо стверджувати, що довжина періоду генератора дорівнює $T = HCK(T_1, T_2, ..., T_n)/2$, де $T_1, T_2, ..., T_n$ – довжини періодів відповідно FCSR--1, FCSR-2,…, FCSR-n, НСК – найменше спільне кратне вказаних чисел. У частинних випадках довжина періоду – $T = HCK(T_1, T_2, ..., T_n)$.

2. Генератор Геффа. FCSR-2,…, FCSR-n є входами мультиплексора, а FCSR-1 керує його виходом (рис.3). Довжина періоду такого генератора дорівнює $T = HCK(T_1, T_2, ..., T_n)$.

Для трьох FCSR вихід генератора Геффа можна описати так: $b = a1 \wedge a2 \oplus \neg a1 \wedge a3$, де $a1, a2, a3$ – виходи FCSR-1, FCSR-2, FCSR-3.

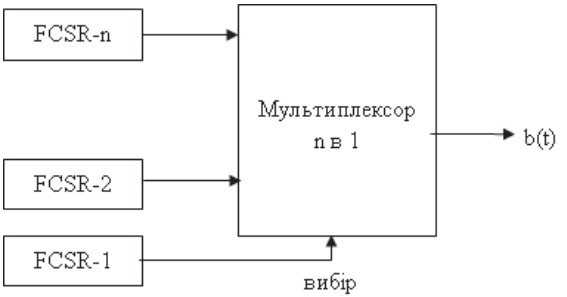

Рис. 3. Генератор Геффа

3. Пороговий (мажоритарний) генератор.

Для даного генератора необхідно використовувати непарну кількість регістрів. Якщо більше половини вихідних бітів FCSR дорівнюють 1, то виходом генератора буде – 1, інакше – 0. Довжина періоду цього ГПВП $T = HCK(T_1, T_2, ..., T_n)$ (рис.4).

Для трьох FCSR вихід генератора можна описати так: $b = a1 \wedge a2 \oplus a1 \wedge a3 \oplus a2 \wedge a3$.

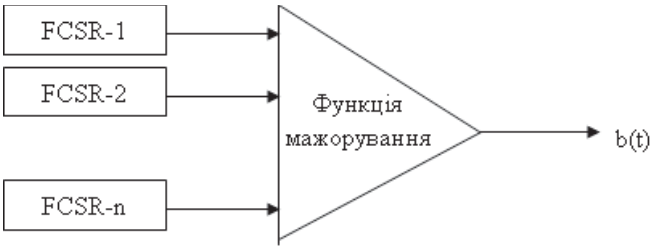

Рис. 4. Пороговий генератор

4. Генератор FCSR із функцією об'єднання – додавання з перенесенням (рис.5).

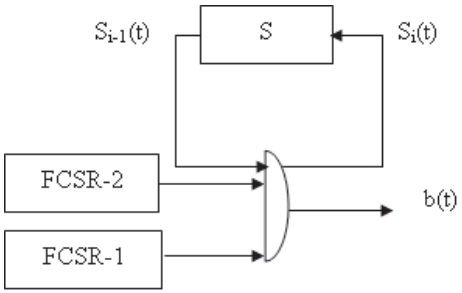

Рис. 5. Генератор додавання з перенесенням

На рис.5 $S_i = a1 \wedge a2 \oplus S_{i-1} \wedge a1 \oplus S_{i-1} \oplus a2$, $b = a1 \oplus a2 \oplus S_{i-1}$. Довжина періоду – $T = HCK(T_1, T_2)$.

5. Генератор «stop-and-go». Використовуються три регістри FCSR. FCSR-2 змінює свій стан, якщо вихід FCSR-1 дорівнює 1, FCSR-3 змінює свій стан у протилежному випадку.

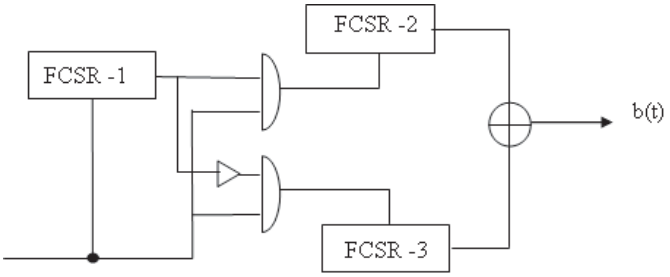

Рис. 6. Генератор «stop-and-go»

На рис.6 представлено структурну схему модифікованого генератора «stop-and-go», де FCSR-2 змінює свій стан, якщо вихід FCSR-1 дорівнює 1, FCSR-3 змінює свій стан, коли вихід FCSR-1 дорівнює 0. Вихід генератора є *xor* FCSR-2 та FCSR-3. Максимальна довжина періоду $T = 2 \cdot HCK(T_1, T_2, T_3)$.

Висновки

Із результатів досліджень генераторів псевдовипадкових послідовностей на основі FCSR бачимо, що використання різних комбінацій FCSR збільшують довжину періоду послідовності. Найкращий період виявився у генераторів побудованих за принципом «stop-and-go». Під час використання значної кількості FCSR можна отримати великі періоди псевдовипадкових послідовностей.

Перспективами подальших досліджень у даному напрямку є використання принципу «stop-and-go» для побудови генератора Голлманна із різною кількістю FCSR та комбінації FCSR/LFSR; проведення комплексної оцінки якості ГПВП з використанням статистичних та графічних тестів; визначення продуктивності побудованих генераторів.

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. *Иванов М. А*. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М.: Изд-во «КУДИЦ-ОБРАЗ», 2003. – 240 с.
3. *Костів Ю. М.* Визначення оптимальних параметрів генератора Голлманна за допомогою статичних тестів NIST / Ю. М. Костів, В. М. Максимович, О. І. Герасимчук, Я. Р. Совин, М. М. Мандрона // Вісник Національного університету «Львівська політехніка», серія «Автоматика, вимірювання та керування». – 2013. – № 753. – С. 57–67.
4. *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.
5. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер.– М. : Триумф, 2002. – 816 с.
6. *Arnault F.* A new class of stream ciphers combining LFSR and FCSR architectures, in Progress in Cryptology / F. Arnault, T. Berger, A. Necer. // INDOCRYPT 2002, ed. by A. Menezes, P. Sarkar. Lecture Notes in Computer Science. – Springer, Berlin, – 2002. – pp. 22–33.
7. *Arnault F*. Design and properties of a new pseudorandom generator based on a filtered FCSR automaton / F. Arnault, T. Berger. – IEEE Trans. Comput. – 2005. – pp. 54, 1374–1383.
8. *Klapper A.* Fibonacci and Galois Representations of Feedback with Carry Shift Registers / A. Klapper, M. Goresky, – IEEE Trans – 2004, pp. 56–71.

Поступила 15.09.2014р.