УДК 004.421.5; 681.3

О. М. Гапак[1]

ПЕРІОД ГЕНЕРАТОРА ГОЛЛМАННА НА ОСНОВІ РЕГІСТРІВ ЗСУВУ ЗІ ЗВОРОТНИМ ЗВ'ЯЗКОМ ЗА ПЕРЕНЕСЕННЯМ

[1]Державний вищий навчальний заклад «Ужгородський національний університет»

Подано результати дослідження генератора Голлманна на основі регістрів зсуву зі зворотним зв'язком за перенесенням. Визначено довжину періоду згенерованих псевдовипадкових послідовностей. Виявлено, як впливає кількість базових компонент та їх порядок у каскаді на період псевдовипадкової послідовності.

Ключові слова: генератор Голлманна, псевдовипадкова послідовність, регістр зсуву та перенесення, період.

Вступ

Генератори псевдовипадкових послідовностей (ГПВП) широко використовуються в різних сферах діяльності: криптографії, імітаційному моделюванні, вимірювальній техніці, розробці комп'ютерних ігор тощо.

Під час використання псевдовипадкових послідовностей (ПВП) у криптографії вимоги до рівномірного розподілу ймовірностей сформованих чисел значно вищі й цим визначається той факт, що у цій галузі з'являється щораз більша кількість нових ідей, підходів [1].

Якісний ГПВП є детермінованим, володіє всіма властивостями істинно випадкових послідовностей і успішно замінює їх, оскільки формування випадкових послідовностей є складним процесом. Під час проектування ГПВП необхідно враховувати низку основних вимог: велика довжина періоду, висока продуктивність алгоритму, простота апаратної та програмної реалізації та інші [2].

Однією з основних характеристик є період ПВП — кількість псевдовипадкових чисел у послідовності, після якої вони починають повторюватись. Довжина періоду послідовності залежить від обраного алгоритму ГПВП, тому під час проектування таких генераторів необхідно враховувати той факт, що період якісної ПВП повинен бути не менше 2^{256} біт.

Існує велика кількість різноманітних методів та принципів генерування ПВП, але найпопулярнішими є генератори, побудовані на регістрах зсуву. У сучасній літературі широко висвітлені дослідження ГПВП на основі регістрів зсуву з лінійним зворотним зв'язком — LFSR (Linear Feedback Shift Register), наведені оцінки їх якості та визначені їх оптимальні параметри. Ці генератори знайшли широке використання в різних галузях науки і техніки. Сучасні дослідження в цій сфері вказують на перспективу використання ГПВП на основі регістрів зсуву зі зворотним зв'язком та перенесення — FCSR (Feedback with Carry Shift Register), які на цей час є малодослідженими.

Ідея використання FCSR є досить новою і вперше подана Енді Клаппером і Марком Горескі [3]. Брюс Шнайер у праці [4] представив загальні ідеї побудови потокових шифрів на базі FCSR. Дослідженням періоду одного FCSR займалися Мартін Міттельбах, Адольф Фінгер [5]. У дослідженнях В. П. Широчина, І. В. Васильцова, Б. З. Карпінського проведено аналіз основного компонента FCSR та визначено максимальний період ГПВП, який побудований на 8 та 9 бітному регістрах зсуву [6]. У статті [7] автор детально описала роботу ГПВП на основі регістрів зсуву зі зворотним зв'язком за перенесенням, розглянуто його комбінації та визначено довжину періодів згенерованих ПВП. Внаслідок чого зроблено висновки про перспективу використання принципу «stop-and-go» для побудови генератора Голлманна на основі FCSR.

Метою роботи є дослідження довжини періоду генератора Голлманна на основі FCSR.

Генератор Голлманна на основі FCSR

Провівши аналіз літературних джерел [4, 8, 9], можемо розширити використання генераторів на основі FCSR, аналогічно до генераторів на основі LFSR.

© О. М. Гапак, 2015

Каскад Голлманна являє собою підсилену версію генератора «stop-and-go». Він складається із деякої послідовності генераторів FCSR, тактування кожного з яких керується попереднім FCSR. Якщо виходом FCSR-1 в момент часу t є 1, то тактується FCSR-2, інакше повторюється попереднє значення FCSR-2. Якщо виходом FCSR-2 в момент часу t є 1, то тактується FCSR-3 і т. д. Вихід останнього FCSR є виходом генератора Голлманна (рис. 1).

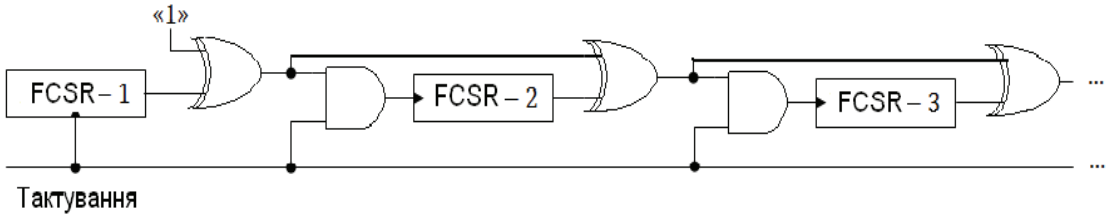

Рис. 1. Каскад Голлманна

Для дослідження періоду ПВП нами розроблений програмний засіб на мові C#. Цей засіб дозволяє згенерувати та визначити період ПВП, яка побудована за алгоритмом Голлманна з різною кількістю базових FCSR та їх порядком розташування у каскаді.

Визначення довжини періоду

Максимальний період одного генератора FCSR дорівнює $q - 1$, де q — ціле число зв'язку, що задає відвідну послідовність. Якщо для n-розрядного регістра відвідна послідовність задана у вигляді (n, m, k, p), то період становитиме $T = 2^n + 2^m + 2^k + 2^p - 2$. З результатів досліджень ГПВП на основі FCSR бачимо, що використання різних комбінацій FCSR збільшують довжину періоду послідовності. Найкращий період спостерігається у генераторів, побудованих за принципом «stop-and-go», максимальна довжина якого $T = 2 \cdot HCK(T_1, T_2, T_3)$ [7].

Спочатку автор дослідила генератор Голлманна з однаковою розрядністю базових регістрів FCSR та однаковою відвідною послідовністю. Під час вибору відвідних послідовностей, що дають максимальний період, за основу взяті дослідження Б. Шнаєра [4].

У роботі розглянуто від трьох до дев'яти регістрів у каскаді Голлманна. Дослідження проводились на регістрах невеликої розрядності — до п'яти біт, а саме: FCSR-1(2,1); FCSR-2(3,2); FCSR-3(3,2,1); FCSR-4(4,2); FCSR-5(4,3,2,1); FCSR-6(5,2,1); FCSR-7(5,4,2,1); FCSR-8(5,4,3,2). Згідно з проведеними експериментами визначено максимальну довжину періоду згенерованих ПВП і представлено її у вигляді залежності від періоду базового FCSR — T (табл. 1).

Таблиця 1

Довжина періоду в залежності від кількості регістрів

Кількість регістрів	Максимальна довжина періоду	Примітка
3	$2T$	—
4	$2T^2$	—
5	$2T^2$	—
6	$12T^2$	Виняток: якщо використовується FCSR-3(3,2,1), то довжина періоду $T = T^3$
7	$12T^2$	—
8	$2T^3$	Виняток: якщо використовується FCSR-3(3,2,1), то довжина періоду $T = T^4$
9	T^4	—

Як бачимо, використання однакових базових регістрів у каскаді Голлманна не є ефективним, на відміну від каскаду Голлманна на основі LFSR з однаковою розрядністю регістрів. Максимальна довжина періоду останнього досягає $T = (2^N - 1)^m$, де $2^N - 1$ — період N-розрядного LFSR, m — кількість базових LFSR. Для обраних автором базових FCSR максимальна довжина періоду становить лише $T^{[m/2]}$. Позитивним фактором є те, що використання більшої кількості регістрів призводить до зростання довжини періоду псевдовипадкової послідовності. Криптографи радять використовувати не менше 15 базових регістрів [8].

Наступні дослідження спрямовані на використання різної розрядності базових FCSR із різними

відвідними послідовностями в каскаді Голлманна. Для експериментів ми обрали дев'ять регістрів розрядності до шести біт: FCSR-1(2,1); FCSR-2(3,2); FCSR-3(3,2,1); FCSR-4(4,2); FCSR-5(4,3,2,1); FCSR-6(5,2,1); FCSR-7(5,4,2,1); FCSR-8(5,4,3,2); FCSR-9(6,2).

Визначимо, як впливає порядок вибору базових регістрів на період ПВП. Наприклад, обравши FCSR-1(2,1); FCSR-2(3,2); FCSR-3(3,2,1) з періодами $T_1 = 4$, $T_2 = 10$, $T_3 = 12$, відповідно, побудуємо шість можливих генераторів Голлманна та визначимо довжини періодів утворених ПВП. Результати дослідження подані у табл. 2, де НСК — найменше спільне кратне вказаних чисел.

Таблиця 2

Довжина періоду в залежності від порядку регістрів

Номер з/п	Послідовність базових регістрів	Довжина періоду T
1	FCSR-1; FCSR-2; FCSR-3	$4\cdot НСК(T_1, T_2, T_3)$
2	FCSR-1; FCSR-3; FCSR-2	$2\cdot НСК(T_1, T_2, T_3)$
3	FCSR-2; FCSR-1; FCSR-3	$2\cdot НСК(T_1, T_2, T_3)$
4	FCSR-2; FCSR-3; FCSR-1	$2\cdot НСК(T_1, T_2, T_3)$
5	FCSR-3; FCSR-1; FCSR-2	$2\cdot НСК(T_1, T_2, T_3)$
6	FCSR-3; FCSR-2; FCSR-1	$4\cdot НСК(T_1, T_2, T_3)$

Із результатів табл. 2 найбільшу довжину періоду отримуємо при виборі послідовності базових FCSR у порядку зростання чи спадання довжини їх періодів. Провівши дослідження над іншими послідовностями регістрів, можемо стверджувати, що базові компоненти потрібно розташовувати в порядку спадання їх періодів. Ці висновки підтверджуються проведеними експериментами та рекомендаціями, наведеними в праці О. І. Гарасимчука [8].

На наступному кроці дослідження визначимо, як впливає кількість та розрядність базових FCSR на період згенерованої ПВП на виході генератора Голлманна. Для експерименту обрано вищевказані регістри FCSR-1…FCSR-9, які розташували в порядку спадання їх періодів. Результати досліджень зведені в табл. 3, де T_i — періоди базових компонент, $i = 1...9$.

Таблиця 3

Довжина періоду в залежності від кількості регістрів різної розрядності

Кількість регістрів	Послідовність базових регістрів	Максимальна довжина періоду
4	FCSR-4 … FCSR-1	$4\cdot НСК(T_4 \dots T_1) = 0{,}72\cdot 10^3$
4	FCSR-6 … FCSR-3	$8\cdot НСК(T_6 \dots T_3) = 2{,}0\cdot 10^3$
5	FCSR-5 … FCSR-1	$4\cdot НСК(T_5 \dots T_1) = 0{,}5\cdot 10^4$
5	FCSR-7 … FCSR-3	$36\cdot НСК (T_7 \dots T_3) = 1{,}2\cdot 10^5$
6	FCSR-6 … FCSR-1	$8\cdot НСК(T_6 \dots T_1) = 0{,}1\cdot 10^5$
6	FCSR-7 … FCSR-2	$36\cdot НСК(T_7 \dots T_2) = 5{,}9\cdot 10^5$
7	FCSR-7 … FCSR-1	$72\cdot НСК(T_7 \dots T_1) = 1{,}2\cdot 10^6$
8	FCSR-8 … FCSR-1	$96\cdot НСК(T_8 \dots T_1) = 4{,}6\cdot 10^7$
9	FCSR-9 … FCSR-1	$>10^8$

Як бачимо із табл. 3, зі збільшенням кількості та розрядності базових компонент довжина періоду генератора Голлманна стрімко зростає. Загальну формулу довжини періоду для ПВП можна представити як $T = k\cdot 10^{m-1}$, де m — кількість базових регістрів, k — дійсне число (при $m \le 6$, $k \in (0; 1]$, якщо $m \ge 7$, $k \in (1; 10)$). Таким чином, максимальна довжина періоду досліджених ПВП сягає 10^m. У першу чергу на період ПВП, побудованої за каскадом Голлманна, впливає довжина періоду базових FCSR: чим більший їх період, тим більший період згенерованої ПВП. Так, наприклад, вибираючи п'ять регістрів FCSR-5…FCSR-1, отримаємо довжину періоду $0{,}5\cdot 10^4$, а вибираючи п'ять регістрів FCSR-7…FCSR-3, довжина періоду становить $1{,}2\cdot 10^5$ (табл. 3). Отже, обираючи регістри більшої розрядності, за однакової їх кількості можна отримати ПВП з максимальним періодом 10^{m+1}.

У роботі [10] автором проведено дослідження якості генератора Голлманна на основі FCSR за допомогою статистичних тестів NIST STS. Аналіз проведених тестувань показав, що цей генератор володіє невисокими статистичними характеристиками і використовувати генератор, побудований тільки на основі FCSR без підключення LFSR у криптографії недоцільно.

Висновки

Таким чином досліджено, як впливає вибір базових компонент генератора Голлманна на довжину періоду псевдовипадкових послідовностей. Так, під час використання однакових регістрів у каскаді Голлманна, максимальна довжина періоду становить $T^{[m/2]}$, де m — кількість базових компонент, T — період базового FCSR. Визначили, що зі збільшенням кількості та розрядності різних базових регістрів отримуємо псевдовипадкову послідовність з максимальною довжиною періоду 10^{m+1}, при цьому вибір компонент повинен здійснюватися у порядку спадання їх періодів.

Перспективами подальших досліджень у цьому напрямку є побудова генераторів на основі комбінації FCSR/ LFSR та проведення оцінки їх якості за допомогою статистичних тестів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Казакова Н. Ф. Проблемы построения комбинированных линейных генераторов псевдослучайных чисел / Н. Ф. Казакова, Ю. В. Щербина // Інформаційна безпека. — 2013. — № 2(10) — С. 58—64.

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

3. Klapper A. Fibonacci and Galois Representations of Feedback with Carry Shift Registers / A. Klapper, M. Goresky. — IEEE Trans. — 2004. — Pp. 56—71.

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

5. Mittelbach M. Investigation of FCSR-based Pseudorandom Sequence Generators for Stream Ciphers / M. Mittelbach, A. Finger // Proc. of International Conference on Networking (ICN), Gosier, Guadeloupe, France, Mar. 2004 . [Електронний ресурс]. — Режим доступу : http://www.researchgate.net/publication/228853356_Investigation_of_FCSR-based_pseudorandom_sequence_generators_for_stream_ciphers/.

6. Shyrochin V. P. Investigations of the basic component of FCSR-generator / V. P. Shyrochin, I. V. Vasyltsov, B. Z. Karpinskij // Computing. — 2003. — Vol. 2, Issue 3, Pp. 77—81. [Електронний ресурс]. — Режим доступу : http://computingonline.net/index.php/computing/article/viewFile/234/209.

7. Гапак О. М. Визначення довжини періоду генераторів псевдовипадкових послідовностей на основі регістрів зсуву зі зворотним зв'язком та перенесення / О. М. Гапак // Моделювання та інформаційні технології. — 2014. — № 73. — С. 92— 97

8. Гарасимчук О. І. Оцінка якості генератора Голлманна, реалізованого на основі модифікованих генераторів М-послідовностей / О. І. Гарасимчук, Ю. М. Костів, Т. Г. Паршенко // Системи обробки інформації. — 2010. — № 6 (87). — С. 35—38.

9. Визначення оптимальних параметрів генератора Голлманна за допомогою статичних тестів NIST / [Ю. М. Костів, В. М. Максимович, О. І. Гарасимчук, Я. Р. Совин, М. М. Мандрона] // Вісник Національного університету «Львівська політехніка». Серія «Автоматика, вимірювання та керування». — 2013. — № 753. — С. 57—67.

10. Гапак О. М. Оцінка якості генератора Голлманна, реалізованого на основі FCSR / О. М. Гапак // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка : зб. наук. пр. — 2015. — № 63. — С. 119—122 .

Рекомендована Центром інформаційних технологій і захисту інформації ВНТУ

Стаття надійшла до редакції 18.09.2015

Гапак Оксана Михайлівна — канд. пед. наук, доцент кафедри комп'ютерних систем та мереж інженерно-технічного факультету, e-mail: oksana.hapak@gmail.com.

Ужгородський національний університету, м. Ужгород

О. М. Hapak[1]

Period of Hollmann Generator on the Basis of Feedback With Carry Shift Registers

[1]Uzhgorod National University

The results of research of Hollmann generator on the basis of feedback with carry shift registers are presented in the article. There has been defined the length of the period of generated pseudorandom sequences. There has been found the impact of quantity of basic components and their order in the cascade for the pseudorandom sequence period.

Keywords: Hollmann generator, pseudorandom sequence, carry shift register, period.

Hapak Oksana M. **—** Cand. Sc. (Education), Assistant Professor of the Chair of Computer Systems and Networks**,** e-mail: oksana.hapak@gmail.com

О. М. Гапак[1]

Период генератора Голлманна на основе регистров сдвига с обратной связью по переносу

[1]Государственное высшее учебное заведение «Ужгородский национальный университет»

Представлены результаты исследования генератора Голлманна на основе регистров сдвига с обратной связью по переносу. Определена длина периода сгенерированных псевдослучайных последовательностей. Выявлено как влияет количество базовых компонент и их порядок в каскаде на период псевдослучайной последовательности.

Ключевые слова: генератор Голлманна, псевдослучайная последовательность, регистр сдвига и переноса, период.

Гапак Оксана Михайловна **—** канд. пед. наук, доцент кафедры компьютерных систем и сетей инженерно-технического факультета, e-mail: oksana.hapak@gmail.com