УДК 004.421.5; 681.3

*ГАПАК О.М.*

# ОЦІНКА ЯКОСТІ ГЕНЕРАТОРА ГОЛЛМАННА, РЕАЛІЗОВАНОГО НА ОСНОВІ FCSR

У статті представлено результати дослідження генератора Голлманна на основі FCSR. Проведено тестування генератора за методикою NIST STS при різній кількості та порядку базових компонент. Показано, що за результатами тестів NIST STS ці генератори не відповідають вимогам, які ставляться до генераторів псевдовипадкових послідовностей.

The results of the research of Hollmann generator on the basis of FCSR are presented in this work. Generator was tested by the technique NIST STS at different quantity and order of the basic components. On the results of NIST STS testing these generators don't meet the requirements that apply to generators of pseudorandom sequences.

## Вступ

У сучасних умовах зростання продуктивності обчислювальних систем та можливостей об'єднання значної кількості комп'ютерів для порушення безпеки даних, актуальною є проблема підвищення надійності захисту інформації, в тому числі засобами, в основі яких лежить використання псевдовипадкових послідовностей (ПВП) [1].

ПВП у криптографії використовуються для генерування ключів симетричних та асиметричних систем; потокового шифрування; генерування електронного цифрового підпису тощо. Розробники генераторів ПВП (ГПВП) повинні дотримуватись ряду вимог: висока швидкодія; якомога більший період повторюваності; простота програмної та апаратної реалізації; можливість керування вхідними параметрами та інші [2].

Найпоширенішими у програмно-апаратній реалізації є ГПВП на основі регістрів зсуву з лінійним зворотним зв'язком – LFSR (Linear Feedback Shift Register). Ці генератори знайшли широке використання у різних галузях науки і техніки. Існує багато методів щодо підвищення їх криптографічних властивостей. До них можна віднести генератор Голлманна, який реалізується на кількох регістрах LFSR. Властивості цих генераторів при правильній реалізації є кращими в порівнянні із генератором LFSR. Результати досліджень таких генераторів Голлманна широко висвітлені у літературі, приведені оцінки їх якості та визначені оптимальні параметри [1; 2; 3]. Проведений аналіз літературних джерел у цій галузі вказує на перспективу використання ГПВП на основі регістрів зсуву зі зворотним зв'язком та перенесення – FCSR (Feedback with Carry Shift Register), які є малодослідженими. В основному всі роботи, присвячені цьому типу генераторів, зводяться до рекомендацій щодо побудови та формального опису принципів їх функціонування [4; 5]. Є декілька досліджень періоду генератора FCSR [6; 7]. У статті [8] ми описали роботу ГПВП на основі FCSR, розглянули його модифікації та прийшли до висновку, що доцільно використати принцип "stop-and-go" для побудови генератора Голлманна. Великий інтерес становить оцінка його якості при різних початкових параметрах.

Метою нашої роботи є проведення оцінки якості генераторів Голлманна на основі FCSR за допомогою статистичних тестів NIST STS, визначення впливу вхідних параметрів базових FCSR на якість генератора та порівняння його із генератором Голлманна, побудованого на основі LFSR.

## Каскад Голлманна на основі FCSR

FCSR схожий на LFSR, в обох є регістр зсуву та функція зворотного зв'язку, різниця полягає в тому, що у FCSR є також регістр перенесення. На рисунку 1 представлена конфігурація 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.

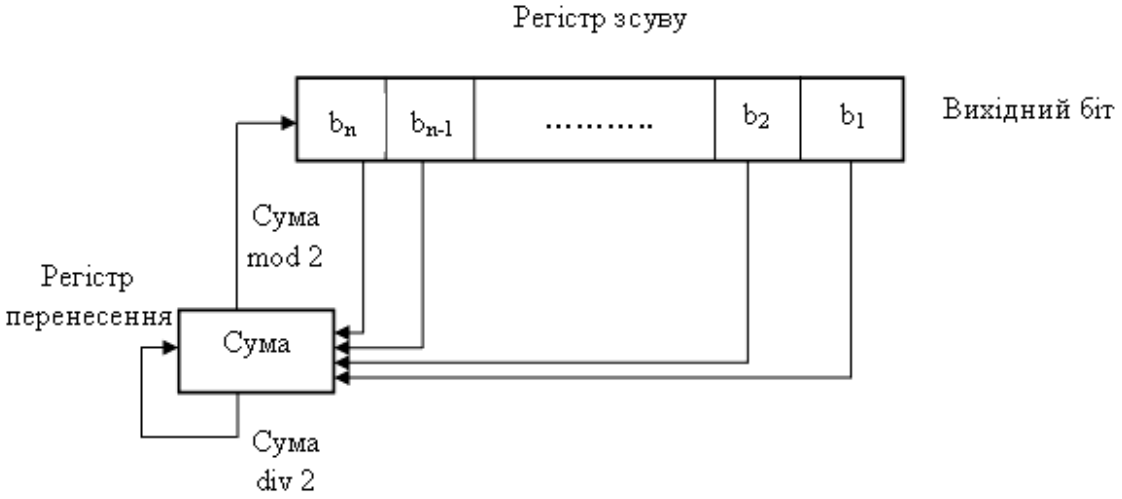


***Рис. 1. FCSR***

Максимальний період 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 $T = 2^n + 2^m + 2^k + 2^p - 2$. Зауважимо, що при використанні $n$-розрядного регістра LFSR максимальний період становить $T = 2^n - 1$.

Проаналізувавши літературу [2; 3; 4; 6], можемо розширити використання генераторів на основі FCSR, аналогічно до генераторів на основі LFSR.

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.2).

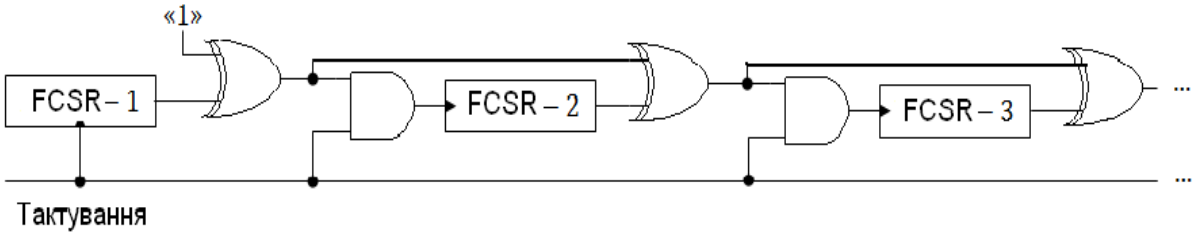


***Рис. 2. Каскад Голлманна***

Для дослідження ГПВП нами розроблений програмний засіб на мові C#. Цей засіб дозволяє згенерувати ПВП за алгоритмом Голлманна із різною кількістю, порядком та довжиною базових FCSR.

Оскільки будь-які послідовності, які породжені ГПВП безпосередньо для криптографічних цілей, підлягають обов'язковому тестуванню, то для проведення оцінки якості генератора Голлманна ми обрали набір статистичних тестів NIST STS.

Статистичні тести NIST STS (National Institute of Standards and Technology Statistical Test Suite) використовуються для визначення якісних та кількісних ознак випадковості послідовності чисел. Сьогодні ця методика є найбільш поширеною серед розробників криптографічних засобів захисту інформації. Пакет NIST STS містить 16 статистичних тестів, які розроблені для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, породжуваних ГПВП. Усі тести спрямовані на виявлення різних дефектів випадковості. Кожен тест подається у розрізі мети, позначення, статистик, опису та правил інтерпретації результатів [9].

Для заданого генератора Голлманна, відповідно до вимог NIST STS, ми сформували двійкові послідовності довжиною $10^8$ біт, для того

щоб із них можна було б отримати 100 підпослідовностей довжиною в 1000000 біт.

Для початку ми визначили, як впливає порядок вибору базових FCSR на статистичні властивості ПВП. Ми обрали три регістри FCSR-1(2,1); FCSR-2(3,2); FCSR-3(3,2,1), сформували шість можливих варіантів генератора Голлманна та провели оцінки якості таких генераторів. Під час вибору базових компонент, що дають максимальний період, ми опиралися на працю Б. Шнаєра [4]. Результати досліджень наведено в таблиці 1.

***Табл. 1. Результати тестування 1***

| Номер з/п | Послідовність базових регістрів | Кількість пройдених тестів |
|---|---|---|
| 1 | FCSR-1; FCSR-2; FCSR-3 | 3 |
| 2 | FCSR-1; FCSR-3; FCSR-2 | 0 |
| 3 | FCSR-2; FCSR-1; FCSR-3 | 1 |
| 4 | FCSR-2; FCSR-3; FCSR-1 | 0 |
| 5 | FCSR-3; FCSR-1; FCSR-2 | 0 |
| 6 | FCSR-3; FCSR-2; FCSR-1 | 3 |

Аналогічні дослідження проведено на регістрах більшої розрядності FCSR-4(6,2); FCSR-5(7,2); FCSR-6(8, 3,2,1). Результати досліджень наведено у таблиці 2.

***Табл. 2. Результати тестування 2***

| Номер з/п | Послідовність базових регістрів | Кількість пройдених тестів |
|---|---|---|
| 1 | FCSR-4; FCSR-5; FCSR-6 | 5 |
| 2 | FCSR-4; FCSR-6; FCSR-5 | 4 |
| 3 | FCSR-5; FCSR-4; FCSR-6 | 4 |
| 4 | FCSR-5; FCSR-6; FCSR-4 | 4 |
| 5 | FCSR-6; FCSR-4; FCSR-5 | 4 |
| 6 | FCSR-6; FCSR-5; FCSR-4 | 5 |

Отже, із одержаних результатів можемо зробити висновки, що на якість генератора впливає порядок вибору базових регістрів. Як бачимо, обирати регістри потрібно у порядку спадання чи зростання їх розрядності та періоду базових FCSR. Ці висновки підтверджують аналогічні дослідження щодо генератора Голлманна на основі LFSR [3].

Далі визначено, як впливає кількість базових FCSR на статистичні властивості ПВП. Для цього ми обрали однакові 3-бітні FCSR(3,2,1) та 7–бітні FCSR(7,4,2,1) із різним початковим вмістом регістрів. У таблиці 3 вказано результати експерименту.

Із результатів проведених експериментів можемо стверджувати, що кількість базових регістрів впливає на статистичні властивості генератора Голлманна, при цьому необхідно використовувати більш як 15 регістрів, що підтверджується рекомендаціями криптологів [3; 4].

***Табл. 3. Результати тестування 3***

| Кількість регістрів | FCSR(3,2,1) | FCSR(7,4,2,1) |
|---|---|---|
| | Кількість пройдених тестів | Кількість пройдених тестів |
| 3 | 1 | 1 |
| 5 | 0 | 2 |
| 7 | 1 | 3 |
| 9 | 1 | 4 |
| 15 | 4 | 4 |
| 19 | 4 | 4 |

Насправді є один суттєвий недолік: використання однакових регістрів FCSR у каскаді Голлманна є неефективним. Так, у дослідженнях генератора Голлманна на основі LFSR із твірним поліномом 7-го степеня кількість пройдених тестів значно більша – уже при використанні п’яти регістрів вона становить 11 [2]. Тому наступні наші дослідження ми проводили із використанням різних базових FCSR у каскаді Голлманна. Для аналізу ми обрали 13-бітні базові регістри із різними відвідними послідовностями та початковим вмістом регістрів. Під час тестувань виявили, що генератор побудований на основі одного FCSR, має кращі статистичні властивості (7 пройдених тестів), а ніж генератор Голлманна (не більше 5 пройдених тестів). Такі дані виявлені й для інших регістрів FCSR.

## Висновки

Аналіз проведених тестувань ПВП побудованої за каскадом Голлманна на основі FCSR, показав, що використання великої кількості базових регістрів приводить до збільшення періоду ПВП. Але, в той же час, згенеровані послідовності не проходять значну частину тестів NIST STS у порівнянні з такими ж генераторами на основі LFSR. Таким чином, на нашу думку, використовувати генератор Голлманна на основі FCSR у криптографії недоцільно.

Перспективами подальших досліджень у цьому напрямку є побудова генератора Голлманна із комбінацією FCSR/LFSR при різних функціях об’єднання; проведення оцінки якості ГПВП з використанням статистичних тестів.

**Список посилань**


1. Зохре Карім Заде. Програмно-апаратні засоби генерації псевдовипадкових послідовностей для підвищення ефективності захисту інформації в ЕОМ та мережах : автореф. дис. на здобуття наук, ступеня канд. техн. наук : спец. 05.13.13 «Обчислювальні машини, системи та мережі» / Зохре Карім Заде. – Київ, 2007. – 18 с.
2. 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.
3. 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.
4. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер.− М. : Триумф, 2002. – 816 с.
5. Klapper A. Fibonacci and Galois Representations of Feedback with Carry Shift Registers / A. Klapper, M. Goresky, – IEEE Trans – 2004, pp. 56–71.
6. 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/.
7. 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: htt -://computingonline.net/index.php/computing/article/viewFile/234/209.
8. 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.
9. NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications//National Institute of Standards and Technology Special Publication 800-22rev1a, 2010, 131 p.