ПОКРАЩЕНИЙ ГЕНЕРАТОР ФІБОНАЧЧІ ДЛЯ ВИКОРИСТАННЯ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Марія Шабатура, Валерія Войтович

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

The statistical characteristics of the classical Fibonacci generator is researched. The generator is proposed to be improved by changing the structural scheme. Was shown the statistical porter of the Fibonacci Generator, which had improved results than classical generator.

Keywords: pseudorandom number generator, information security systems, statistical characteristics, test NIST.

Для забезпечення безпеки комп'ютерних систем критично важливо мати алгоритми, що задовольняють такому критерію як непередбачуваність. Іншими словами, навіть знаючи алгоритм генератора й всі попередні елементи послідовності, повинне бути максимально трудомістким обчислення наступних елементів. Потреби в потужних наукових обчислювачах набагато обганяють можливості вдосконалювання складних архітектур багатопроцесорних систем, і, що головне, ці потреби дуже погано узгоджуються з реальними бюджетами наукових організацій. Як не дивно, але в обох ситуаціях роль генератора псевдовипадкових чисел украй важлива. Характеристики систем безпеки здебільшого залежать від характеристик їхніх криптографічних підсистем, які визначаються не тільки алгоритмікою, але і якісними показниками саме використовуваних ГПВЧ або апаратних генераторів випадкових чисел.

Під час дослідження класичного генератора Фібоначчі підтвердився відомий факт про незадовільні статистичні характеристики, що свідчить про не випадковість послідовностей, які генеруються такими генераторами.

Рівняння роботи класичного генератора Фібоначчі

$$x_i = (x_i + x_{i-1}) \bmod m \tag{1}$$

На рис. 1 наведено статистичний портрет класичного генератора Фібоначчі.

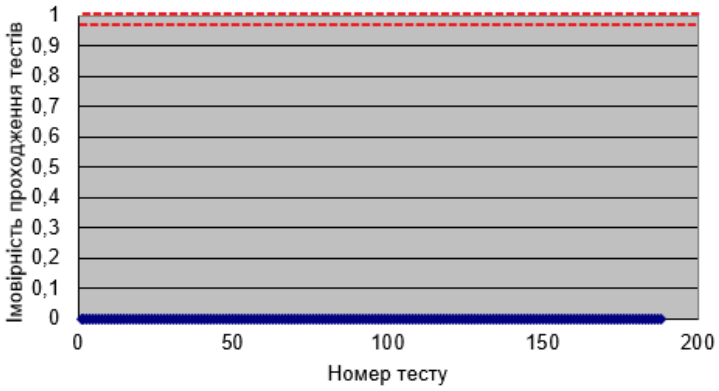

Рис. 1. Статистичний портрет класичного генератора Фібоначчі

Для покращення статистичних характеристик, було побудовано модифікований генератор Фібоначчі шляхом доповнення рівняння (1), додаванням половини першого регістру. Покращений генератор буде містити, регістри x, x1, x2, два комбінаційні суматори КС (рис. 2). На виході МГФ формується послідовність ПВЧ відповідно до виразу:

$$x_i = (x_i + x_{i-1} + x_i / 2) \bmod m \tag{2}$$

де x – значення у регістрах.

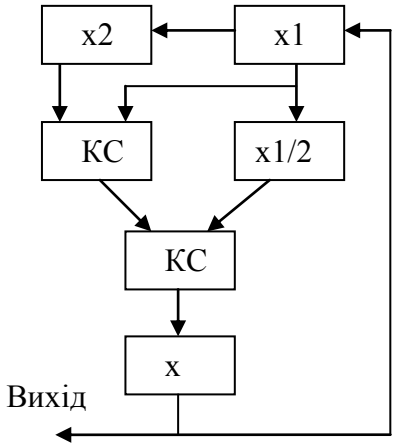

Рис. 2. Структурна схема модифікованого генератора Фібоначчі

На рис. 3 наведено отримані статистичні характеристики бітової послідовності з виходу покращеного генератора. Усі дослідження здійснювалися з допомогою американського набору статистичних тестів NIST [3].

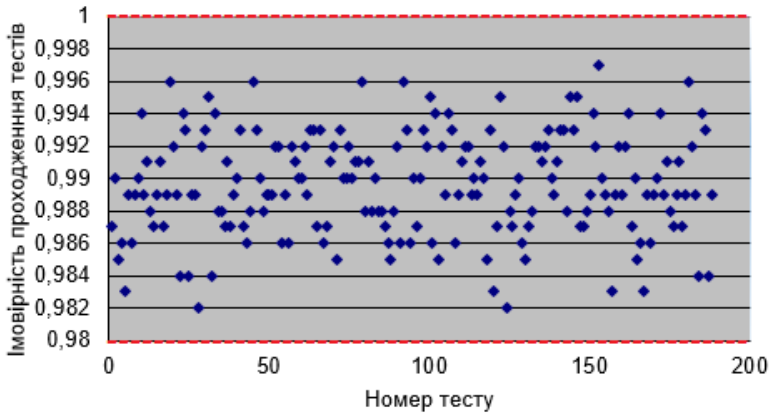

Рис. 3. Статистичний портрет класичного генератора Фібоначчі

Із рис. 3 видно, що всі тести успішно пройдено, всі значення тестів потрапили в межі довірчого інтервалу, який позначено двома пунктирними лініями. Це означає, що запропонований варіант удосконалено генератора Фібоначчі генерує послідовність, яка відповідає вимогам випадковості.

За результатами проведених досліджень можна зробити висновок, що основним чинником, який дозволив істотно покращити статистичні характеристики ГПВЧ, побудованого на основі класичного генератора Фібоначчі, є додавання до їх структури половини попереднього значення.

Література

1. Иванов, М.А. Криптографические методы защиты информации / М.А. Иванов.- М.: КУДИЦ-ОБРАЗ, 2012.-368с.
2. Mandrona M.M. Investigation of the Statistical Characteristics of the Modified Fibonacci Generators / M.M. Mandrona, V.M. Maksymovych // Journal of Automation and Information Sciences 10.1615/JAutomatInfScien.v46.i12.60 pages 48-53
3. NIST SP80022. A statistical Test Suite of Random and Pseudorandom Number Generators for Cryptographic Applications: [Електронний ресурс]. April 2000. Доступний з: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf.
4. Implementation of modified additive lagged Fibonacci generator / Mandrona M.M., Maksymovych V.M., Harasymchuk O.I., Kostiv Yu.M. // Challenges of Modern Technology, Vol. 7, No 1, 2016, Pp. 3-6
5. Generator of pseudorandom bit sequence with increased cryptographic security / [M.M. Mandrona, V.M. Maksymovych, Yu.M. Kostiv, O.I. Harasymchuk] // Metallurgical and Mining Industry: scientific and technical journal – 2014. – No. 5. – Pp. 25-29