ДОСЛІДЖЕННЯ АДИТИВНИХ ГЕНЕРАТОРІВ ФІБОНАЧЧІ ДЛЯ ЗАСТОСУВАННЯ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Марія Мандрона, Білан Віра

Львівський державний університет безпеки життєдіяльності, м. Львів, Україна

In the paper was researching modified version of the additive Fibonacci generator and was proposing a new algorithms of generators which have improved statistical characteristics.

Keywords: generator of pseudorandom bit sequence, a statistical security, protection of information.

У сучасному інформатизованому світі псевдовипадкові числа широко використовуються в різних галузях науки і техніки, зокрема, у системах захисту інформації, у сучасних телекомунікаційних системах, у вимірювальній техніці. У сфері захисту інформації псевдовипадкові числа використовують для потокового шифрування каналів зв'язку, генерування ключів для криптосистем, хешування інформації, формування цифрового підпису, а також для створення різного роду зашумлень і т.д. Встановлено, що характеристики систем безпеки залежать від характеристик їх криптографічних підсистем, які визначаються не тільки використаними алгоритмами, але й якісними показниками використаних псевдовипадкових послідовностей. Оскільки безпека криптосистеми зосереджена на ключі, то при використанні ненадійного процесу генерації ключів, вся криптосистема стає вразливою [1].

У багатьох працях проводилось дослідження роботи і статистичних характеристик адитивних генераторів Фібоначчі [1-3]. При цьому були виявленні варіанти їх побудови, що забезпечують високу якість, однак більшість з них орієнтовані на програмну реалізацію. В цій роботі акцентується увага на знаходженні нових алгоритмів роботи генераторів Фібоначчі із забезпеченням задовільних статистичних характеристик з можливістю апаратної реалізації, яка б забезпечувала високу швидкодію роботи.

Метою роботи є дослідження модифікованої версії адитивного генератора Фібоначчі та знаходження нових алгоритмів роботи генераторів із забезпеченням задовільних статистичних характеристик з можливістю подальшої апаратної реалізації.

Адитивні генератори Фібоначчі є генераторами псевдовипадкових чисел, однак, вони одночасно можуть функціонувати і як генератори псевдовипадкових бітових послідовностей, що формуються на виходах окремих розрядів регістрів пам'яті [3].

Найбільш простий адитивний генератор Фібоначчі функціонує за алгоритмом:

$$X_{j+1} = (X_j + X_{j-1}) \bmod M, \quad (1)$$

де X_j, X_{j-1} – значення чисел у регістрах, M – просте число

На генераторів формуються послідовності псевдовипадкових чисел у відповідності до виразів:

$$X_{j+1} = (X_j + X_{j-1} + a) \bmod m \quad (2)$$

$$X_{j+1} = (X_j + X_{j-1} + X_{j-2} + a) \bmod m \quad (3)$$

$$X_{j+1} = (X_j + X_{j-1} + X_{j-2} + X_{j-3} + a) \bmod m \quad (4)$$

$$X_{j+1} = (X_j + X_{j-1} + X_{j-2} + X_{j-3} + X_{j-4} + a) \bmod m \quad (5)$$

де $m=2^s$, s – кількість двійкових розрядів структурних елементів. Значення змінної a визначається логічним рівнянням [2-3]:

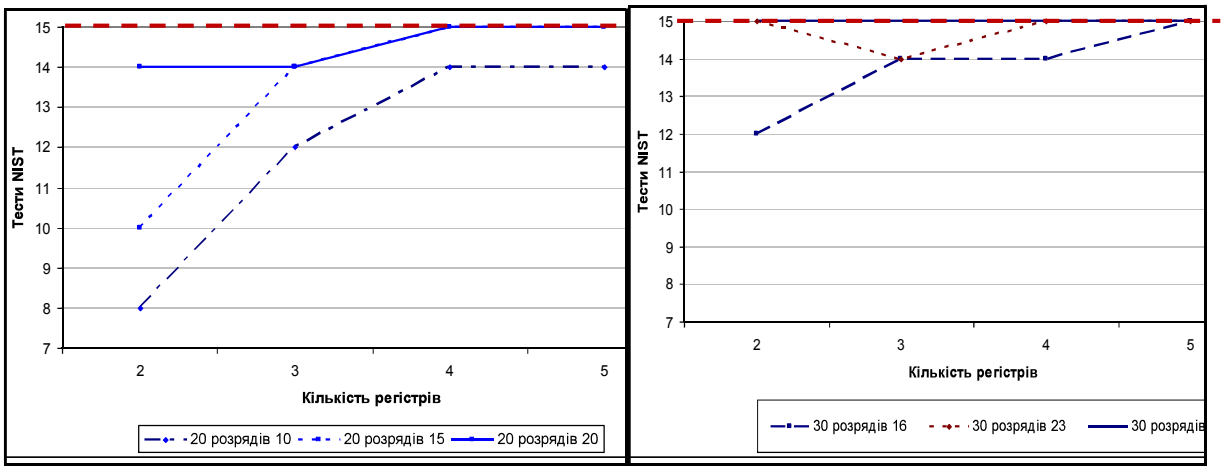
$$a = a_0 \ \text{xor} \ a_1 \ \text{xor} \ a_2 \ \text{xor} \ \cdots \ \text{xor} \ a_z, \quad (6)$$

де s – кількість двійкових розрядів, a_i ($i = 0, 1,\ldots, s$). Кількість членів рівняння (6) може вибиратись з діапазону 0 … s.

Дослідження генераторів здійснювалось з використанням методики NIST. Вважається, що якщо досліджувана послідовність успішно пройшла усі 15 статистичних

тести, тоді робиться висновок, що така послідовність дійсно випадкова, отже її можна використовувати для побудови систем захисту інформації. Якщо ж хоча б один тест не пройдено, тоді вважається, що послідовність не відповідає вимогам випадковості.

На рис. 1*а* і *б* наведено залежності, які відображають вплив кількості структурних елементів на проходження тестів NIST. Кожна послідовність тестувалась 15 тестами [2] на графіках представлено результати тестування (для зручності межу проходження тестів позначено пунктирною лінією). На рис. 1*а* наведено результати дослідження генератора з такими параметрами: кількість двійкових розрядів – 20 біт із трьома варіантами значення змінної *a*, відповідно 10, 15 і 20 біт. На рис. 1*б* дослідження генератора з параметрами: кількість двійкових розрядів – 30 біт із трьома варіантами значення змінної *a*, відповідно 16, 23 і 30 біт.



а *б*

Рис. 1. Залежність проходження тестів NIST від кількості структурних елементів

Отже, за результатами проведених досліджень, як висновок можна підсумувати:

✓ збільшення кількості розрядів структурних елементів ГПВП позитивно впливає на статистичні характеристики;

✓ введення логічної схеми у структуру генератора призводить до збільшення періоду повторення генератора, а також до покращення статистичних характеристик згенерованих послідовностей;

✓ використання логічної схеми дає змогу, в якості модуля, використовувати степінь двійки, що дозволить значно спростити апаратну реалізацію генератора Фібоначчі;

✓ якщо кількість членів використаних у рівнянні (6), реалізованого в логічній схемі, є меншою, ніж половина кількості розрядів структурних елементів, то статистичні характеристики вихідних згенерованих послідовностей є незадовільними.

Література

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванов, И.В. Чугунков : под ред. М.А. Иванова. – М. : НИЯУ МИФИ, 2012. – 400 с.
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. Костів Ю.М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі / Костів Ю.М., Максимович В.М., Гарасимчук О.І., М.Мандрона М.М. // Комп'ютерні технології друкарства : збірник наукових праць. – Львів : Вид-во Української академії друкарства. – 2013. – № 29. – С. 167-174.