УДК 004.421.5:[519.246+512.624.95
DOI: 10.31673/2409-7292.2024.020008

Кіх М. В., Нємкова О. А.

ПОКРАЩЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ МОДИФІКОВАНОГО АДИТИВНОГО ГЕНЕРАТОРА ФІБОНАЧЧІ

Псевдовипадкові бітові послідовності (ПВБП) відіграють ключову роль у багатьох областях інформаційної безпеки, криптографії та комп'ютерних наук. Покращення статистичних характеристик ПВБП допомагає зробити їх більш випадковими, що важливо для безпеки і надійності в різних сферах застосування. Ця стаття присвячена дослідженню статистичних характеристик псевдовипадкових бітових послідовностей модифікованого адитивного генератора Фібоначчі при змінних значеннях модуля і початкового числа в регістрах. Для тестування статистичних характеристик нами було використано набір тестів NIST. Результати дослідження показують, що зміна значень модулів і початкових чисел в регістрах по-різному впливає на якість та стійкість згенерованих послідовностей. При використанні невеликих значень модуля та початкового числа в регістрах генератор не характеризується повною статистичною безпекою, але збільшення цих параметрів призводить до покращення ефективності та якості генератора. Представлені результати підтверджують, що до покращень статистичних характеристик МАГФ призвело збільшення значень модуля m. Збільшення початкового числа в регістрах x_0 мало незначний вплив на проходження тестів NIST. Було встановлено конкретні значення модуля та початкового числа в регістрах, при яких МАГФ успішно пройшов усі тести NIST. Отримані результати можуть мати практичне застосування у розробці криптографічних систем та в інших областях, де важлива випадковість генерованих даних.

Ключові слова: інформаційна безпека, псевдовипадкова бітова послідовність, модифікований адитивний генератор Фібоначчі, тести NIST, статистичний портрет.

Вступ

Псевдовипадкові бітові послідовності (ПВБП) відіграють ключову роль у багатьох областях інформаційної безпеки, криптографії та комп'ютерних наук. Ось деякі аспекти їх важливості [1–8]:

1. Криптографія. ПВБП використовуються для створення ключів шифрування [1, 2]. Без випадкових елементів ключі можуть стати передбачуваними і легко піддаватися атакам. ПВБП використовуються для генерації випадкових чисел при встановленні сесійних ключів для забезпечення безпеки під час обміну даними між користувачами або системами [4].

2. Системи безпеки. Важливі для генерації ключів, які використовуються в протоколах безпеки, таких як TLS, IPsec тощо. Використовуються для створення випадкових ідентифікаторів або паролів, які важко вгадати [4, 5].

3. Моделювання та тестування. У наукових дослідженнях і в розробці ПВБП використовуються для створення випадкових обставин або подій для моделювання різних сценаріїв [6, 7]. Випадкові послідовності важливі для проведення об'єктивних тестів програм, таких як тестування на витривалість або випадкове тестування.

4. Машинне навчання. У деяких алгоритмах нейронних мереж ПВБП використовуються для ініціалізації ваг для уникнення проблеми затухання або вибуху градієнтів [3]. Використовуються для створення штучних даних для тренування моделей.

5. Статистика та наукові дослідження. У наукових дослідженнях випадкові послідовності використовуються для проведення контрольних випробувань [1, 2, 8].

Загалом, покращення статистичних характеристик ПВБП допомагає зробити їх більш випадковими, що важливо для безпеки і надійності в різних сферах застосування. Вони відіграють ключову роль у створенні систем, які можуть стійко відстояти атакам та забезпечувати випадковість, яка часто є необхідною в різних обчислювальних задачах.

Постановка проблеми

Статистична безпека псевдовипадкових бітових послідовностей, які використовуються у багатьох областях інформаційної безпеки та криптографії, є дуже важливою [1-8]. Модифіковані адитивні генератори Фібоначчі (МАГФ) широко використовуються для

створення таких послідовностей. Проте, ефективність та надійність МАГФ часто піддаються сумнівам через недостатню випадковість їхніх вихідних послідовностей [9, 10].

Одним із методів оцінки випадковості є використання статистичних тестів, таких як тести, розроблені Національним інститутом стандартів і технологій (NIST) [11]. Вони дозволяють об’єктивно оцінити рівень випадковості псевдовипадкових послідовностей та виявити можливі вразливості у генераторах.

Аналіз наукових публікацій. Роботи [1, 9, 10] знайомлять нас із принципами роботи адитивного генератора Фібоначчі (АГФ), але не дозволяють об'єктивно оцінити рівень випадковості псевдовипадкових послідовностей при зміні значень модулів і початкових чисел в регістрах.

У роботах [2, 4] були розглянуті дослідження, що стосуються аналізу псевдовипадкових послідовностей звичайного АГФ. Проте вони обмежені за обсягом і глибиною аналізу. Це призводить до недостатньої уваги до певних аспектів випадковості.

У роботах [3-8] досліджені перспективи і можливості застосування МАГФ та звичайного АГФ, але відсутнє оцінювання статистичної безпеки згенерованих ПВБП.

У роботах [9, 10] використовуються тести NIST для оцінки випадковості псевдовипадкових послідовностей МАГФ. Не існує загальноприйнятих стандартів або методів оцінки випадковості МАГФ. Це призводить до різних підходів аналізу та інтерпретації результатів, що ускладнює порівняння різних досліджень. Результати аналізу псевдовипадкових послідовностей МАГФ є варіабельними залежно від параметрів генератора (не враховувались зміни значень модулів і початкових чисел в регістрах) та методів тестування, що використовуються. Це створює непевність у відносності випадковості послідовностей. Порівняння результатів власних експериментів з результатами цих досліджень дозволить обґрунтувати нові підходи і покращення.

У роботі [11] представлена методика тестування NIST для оцінки випадковості псевдовипадкових послідовностей. Даний набір статистичних тестів надає доступ до різноманітних тестів, що охоплюють різні аспекти випадковості, такі як рівномірність розподілу, автокореляція, середнє відхилення тощо. Це дозволяє отримати комплексну оцінку випадковості послідовності. Тестовий пакет NIST є відкритим і доступним для всіх, хто бажає використовувати його для оцінки випадковості псевдовипадкових послідовностей. Крім того, NIST надає детальну документацію, яка пояснює кожен тест та його використання. Інші наявні тести (TestU01, DIEHARD тощо) не охоплюють більшість аспектів випадковості і не надають детальну документацію. Беручи до уваги все перераховане, для дослідження МАГФ було вибрано набір статистичних тестів NIST.

Метою статті є дослідження можливості покращення статистичних характеристик псевдовипадкових бітових послідовностей модифікованого адитивного генератора Фібоначчі шляхом зміни значень модулів і початкових чисел в регістрах.

Модифікований адитивний генератор Фібоначчі. На рис. 1 наведена структурна схема генератора ПВБП на основі модифікованого адитивного генератора Фібоначчі [1, 2], що працює у відповідності до рівняння

$$X_i = (X_{i-8} + X_{i-3} + hhh) \bmod m.$$

До його складу входять регістри $Рг_1$ – $Рг_8$, комбінаційний суматор КС (що реалізує функцію mod m) і логічна схема ЛС, що реалізує логічне рівняння

$$hhh = h_0 \text{ xor } h_1 \text{ xor } h_2 \text{ xor } h_3,$$

де h_0, h_1, h_2, h_3 – значення двійкових розрядів числа X_{i-1} [4].

Робота генератора описується рівняннями:

$$X_{i-8} = X_{i-7},\ X_{i-7} = X_{i-6},\ X_{i-6} = X_{i-5},\ X_{i-5} = X_{i-4},\ X_{i-4} = X_{i-3},\ X_{i-3} = X_{i-2},\ X_{i-2} = X_{i-1},\ X_{i-1} = X_i,$$
$$X_i = (X_{i-8} + X_{i-3} + hhh) \bmod m.$$

Вихідна ПБВП формується на виході молодшого розряду b_i.

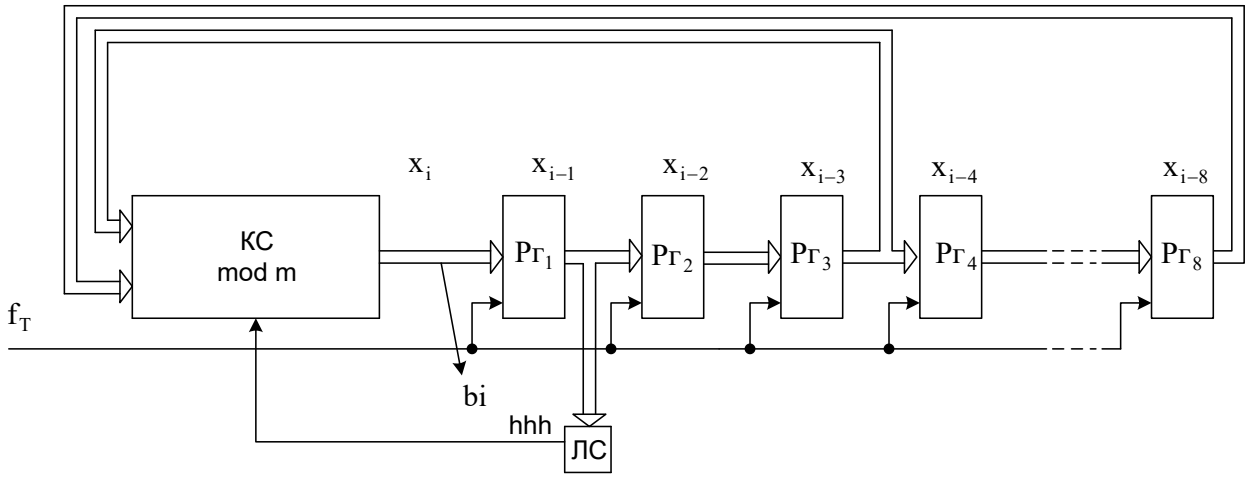


Рис. 1. Генератор ПВБП на основі модифікованого адитивного генератора Фібоначчі, що працює відповідно рівняння $X_i = (X_{i-8} + X_{i-3} + hhh) \bmod m$

Дослідження вихідних послідовностей МАГФ за допомогою пакету тестів NIST. У програмі, що імітує роботу генератора (структурна схема наведена на рис. 1), необхідними вхідними даними є модуль m і початкове число в регістрах x_0 для обчислення значень X_i – X_{i-8} в регістрах $Рг_1$ – $Рг_8$ [6]. Автори статті вважають, що потрібно визначити, які оптимальні значення m і x_0 забезпечать статистичну безпеку МАГФ.

Застосовуючи набір статистичних тестів NIST [3, 5], було проаналізовано кілька варіацій створення модифікованих адитивних генераторів Фібоначчі при змінних значеннях модуля m і початкового числа в регістрах x_0, а саме:

1. m = 3, 11 і фіксованому значенню початкового числа в регістрах x_0 = 7.
2. m = 59, 107 і фіксованому значенню початкового числа в регістрах x_0 = 53.
3. m = 349, 653 і фіксованому значенню початкового числа в регістрах x_0 = 97.
4. m = 997, 2027, 3527 і фіксованому значенню початкового числа в регістрах x_0 = 151.
5. x_0 = 331, 593 і фіксованому значенню модуля m = 89.
6. x_0 = 1009, 2017, 3499 і фіксованому значенню модуля m = 149.
7. m = 3617 і x_0 = 3; m = 3613 і x_0 = 3571.

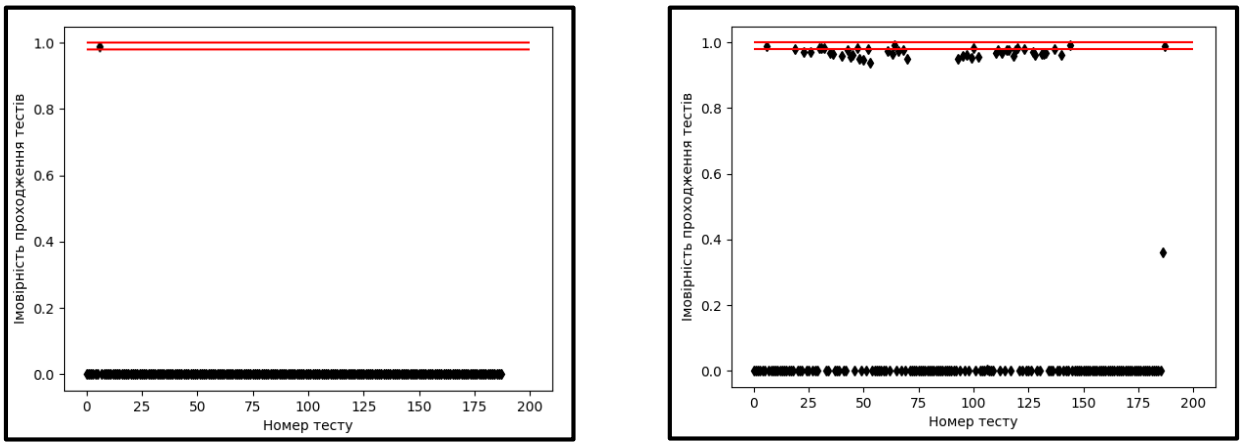
Всі значення модуля і початкового числа в регістрах були вибрані з множини простих чисел.

Результати тестування представлені на рис. 2–8 у вигляді статистичних портретів. На горизонтальній вісі зображено номер тесту NIST, а на вертикальній вісі – імовірність успішного проходження тесту. Тест вважається успішно пройденим, якщо імовірність потрапляє в інтервал від 0,98 до 0,998; в іншому випадку тест вважається не пройденим [5]. Межі довірчого інтервалу відзначені червоними лініями для кращого візуального сприйняття [3].

На рис. 2 наведені результати тестування МАГФ у вигляді статистичних портретів. При m = 3, x_0 = 7 було пройдено 1 тест із 188 (рис. 2 а). Для m = 11, x_0 = 7 пройдено 13 тестів (рис. 2 б).

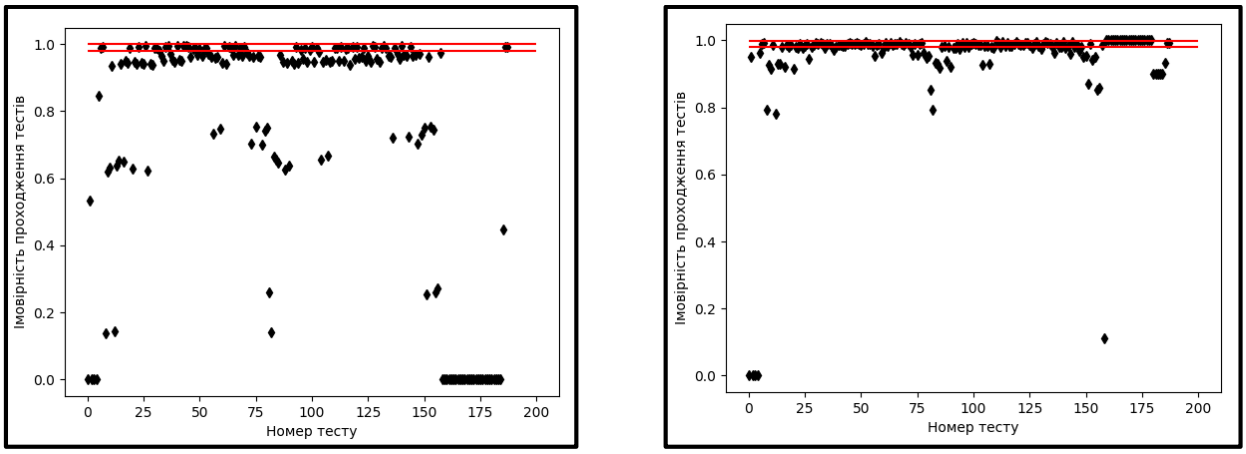
На рис. 3 наведені результати тестування МАГФ у вигляді статистичних портретів. При m = 59, x_0 = 53 було пройдено 49 тестів із 188 (рис. 3 а). Для m = 107, x_0 = 53 пройдено 121

тест (рис. 3 б). Отже, представлене збільшення значень модуля m і початкового числа в регістрах x_0 призвело до покращення статистичних характеристик МАГФ.



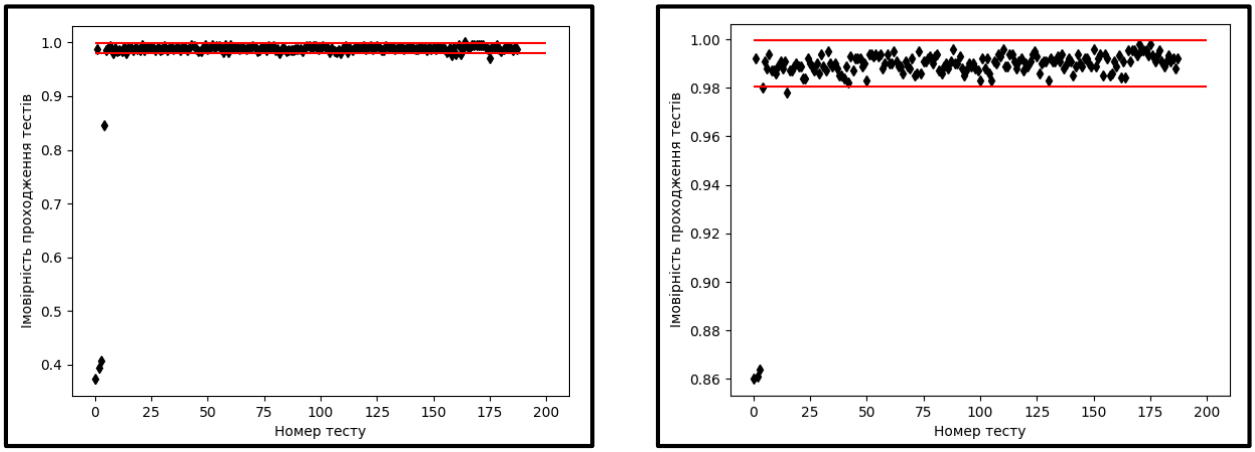
а б

Рис. 2. Статистичні портрети модифікованих адитивних генераторів Фібоначчі при x_0 = 7: а – варіант при m = 3; б – варіант при m = 11



а б

Рис. 3. Статистичні портрети модифікованих адитивних генераторів Фібоначчі при x_0 = 53: а – варіант при m = 59; б – варіант при m = 107

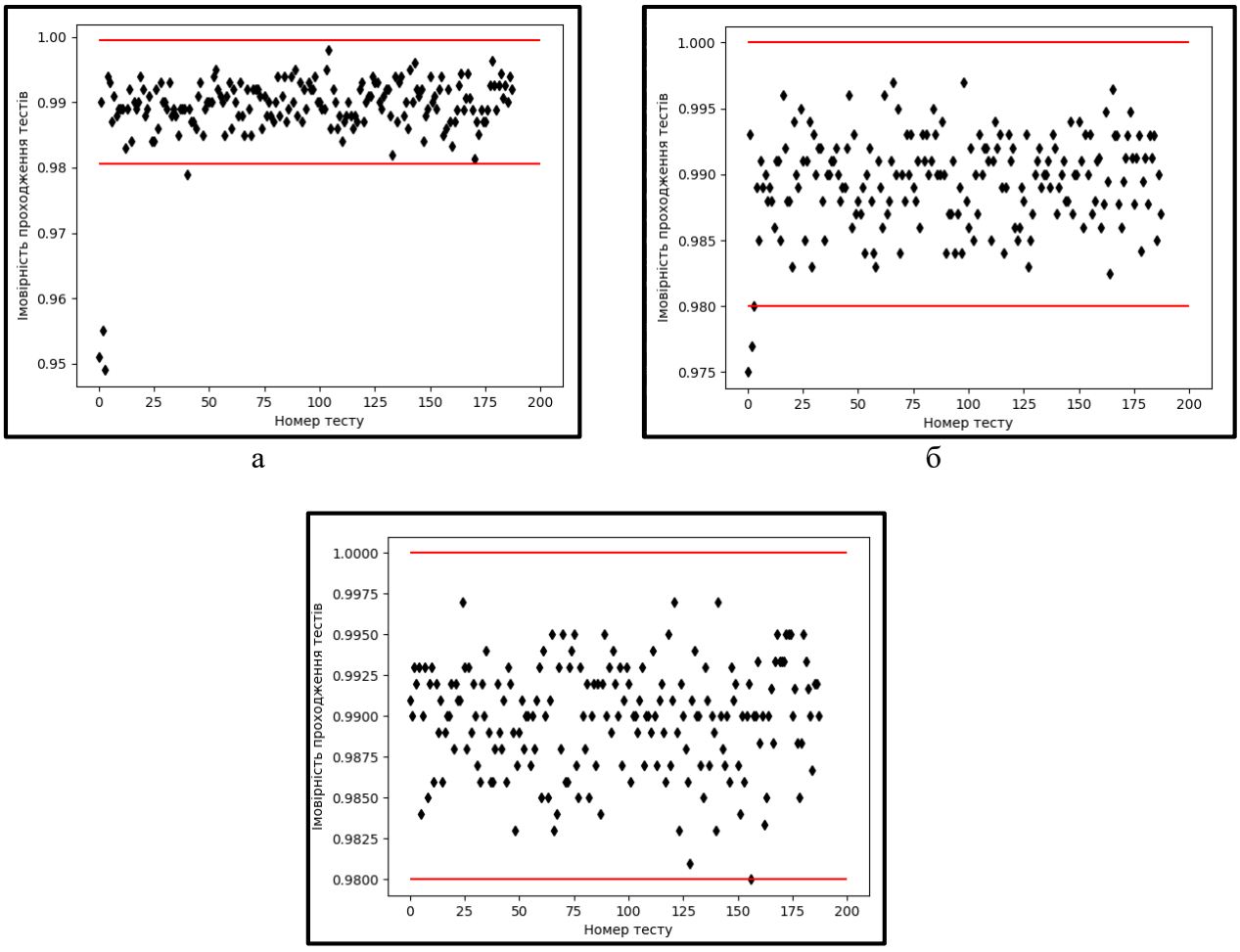


а б

Рис. 4. Статистичні портрети модифікованих адитивних генераторів Фібоначчі при x_0 = 97: а – варіант при m = 349; б – варіант при m = 653

На рис. 4 наведені результати тестування МАГФ у вигляді статистичних портретів. При m = 349, x_0 = 97 було пройдено 180 тестів із 188 (рис. 4 а). Для m = 653, x_0 = 97 пройдено 184 тести (рис. 4 б). Отже, представлене збільшення значень модуля m і початкового числа в регістрах x_0 призвело до значних покращень статистичних характеристик МАГФ.

На рис. 5 наведені результати тестування МАГФ у вигляді статистичних портретів. При m = 997, x_0 = 151 було пройдено 184 тести із 188 (рис. 5 а). Для m = 2027, x_0 = 151 пройдено 186 тестів (рис. 5 б) і для m = 3527, x_0 = 151 пройдено 188 тестів із 188 (рис. 5 в). Отже, представлене збільшення значень модуля m і початкового числа в регістрах x_0 призвело до значних покращень статистичних характеристик МАГФ. Вдалося досягнути результату, коли усі тести було пройдено.



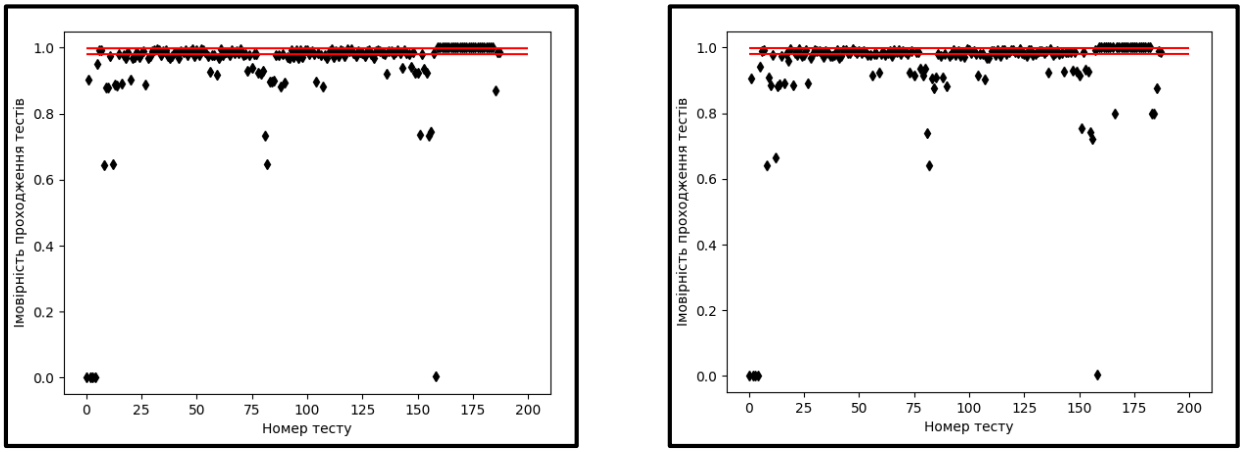
а б в

Рис. 5. Статистичні портрети модифікованих адитивних генераторів Фібоначчі при x_0 = 151: а – варіант при m = 997; б – варіант при m = 2027; в – варіант при m = 3527

На рис. 6 наведені результати тестування МАГФ у вигляді статистичних портретів. При x_0 = 331, m = 89 було пройдено 103 тести із 188 (рис. 6 а). Для x_0 = 593, m = 89 пройдено 107 тестів (рис. 6 б).

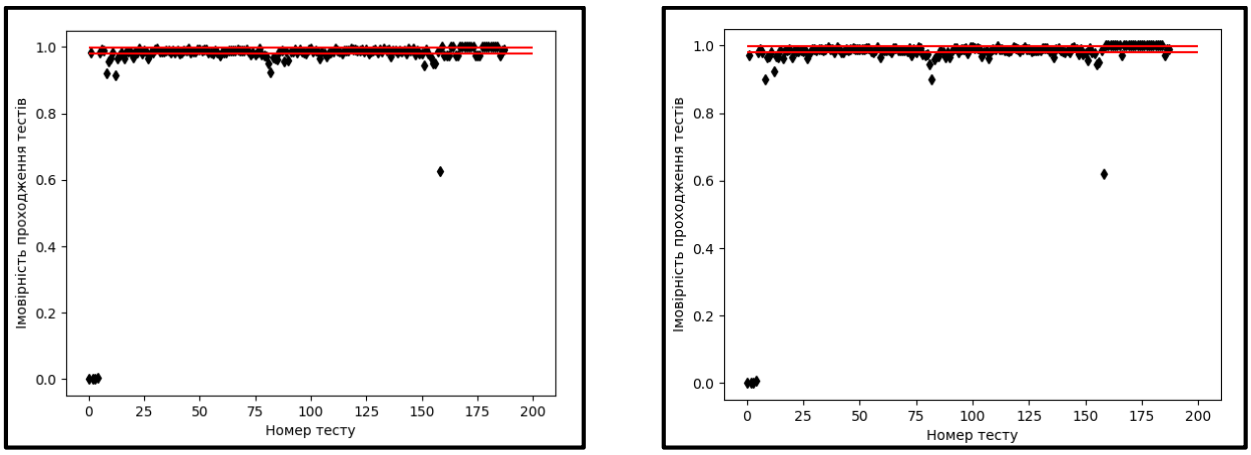
На рис. 7 наведені результати тестування МАГФ у вигляді статистичних портретів. При x_0 = 1009, m = 149 і x_0 = 2017, m = 149 було пройдено по 139 тестів із 188 відповідно для кожного варіанту (рис. 7 а, б). Для x_0 = 3499, m = 149 пройдено 143 тести із 188 (рис. 7 в). Отже, можна зробити висновок, що до покращень статистичних характеристик МАГФ

призвело збільшення значень модуля m. Збільшення початкового числа в регістрах x_0 мало незначний вплив на проходження тестів NIST.

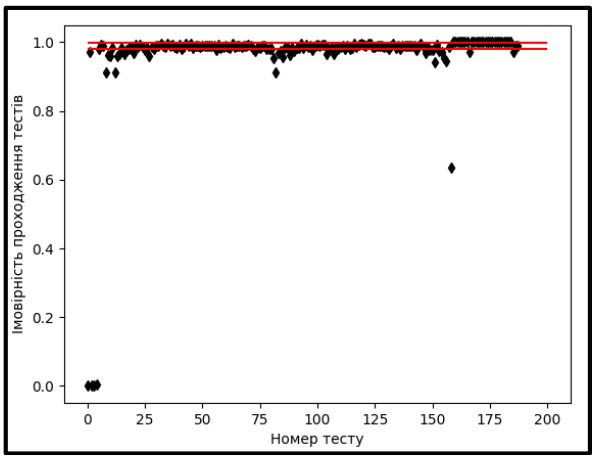


а б

Рис. 6. Статистичні портрети модифікованих адитивних генераторів Фібоначчі при m = 89: а – варіант при x_0 = 331; б – варіант при x_0 = 593

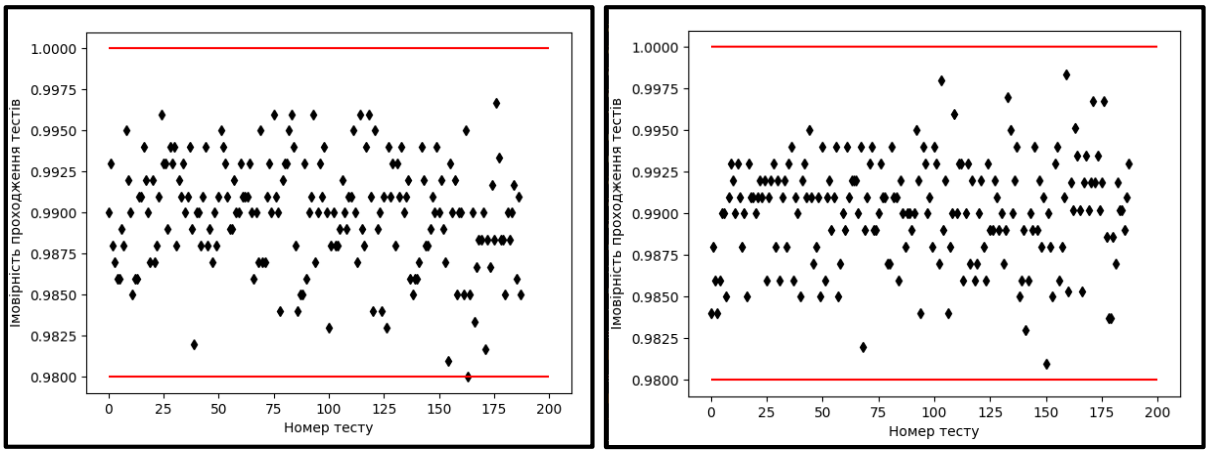


а б



в

Рис. 7. Статистичні портрети модифікованих адитивних генераторів Фібоначчі при m = 149: а – варіант при x_0 = 1009; б – варіант при x_0 = 2017; в – варіант при x_0 = 3499



а б

Рис. 8. Статистичні портрети модифікованих адитивних генераторів Фібоначчі: а – варіант при m = 3617, x_0 = 3; б – варіант при m = 3613, x_0 = 3571

На рис. 8 наведені результати тестування МАГФ у вигляді статистичних портретів. При m = 3617, x_0 = 3 було пройдено 188 тестів із 188 (рис. 8 а). Для m = 3613, x_0 = 3571 пройдено 188 тестів (рис. 8 б).

В таблицях 1 та 2 наведено результати проходження тестів, також наведено період ПВБП.

Таблиця 1

Вплив значення модуля m на кількість пройдених тестів

m	x_0	Кількість пройдених тестів з 188	Кількість не пройдених тестів з 188	Період ПВБП
3	7	1	187	5274
11		13	175	74111475
59	53	49	139	$> 10^9$
107		121	67	$> 10^9$
349	97	180	8	$> 10^9$
653		184	4	$> 10^9$
997	151	184	4	$> 10^9$
2027		186	2	$> 10^9$
3527		188	0	$> 10^9$

Таблиця 2

Вплив початкового числа в регістрі x_0 на кількість пройдених тестів

x_0	m	Кількість пройдених тестів з 188	Кількість не пройдених тестів з 188	Період ПВБП
3	3617	188	0	$> 10^9$
331	89	103	85	$> 10^9$
593		107	81	$> 10^9$
1009	149	139	49	$> 10^9$
2017		139	49	$> 10^9$
3499		143	45	$> 10^9$
3571	3613	188	0	$> 10^9$

Період ПВБП при m = 3, x_0 = 7 становить 5274. Для m = 11, x_0 = 7 період становить 74111475. Для решти значень модулів і початкових чисел в регістрах період більший 10^9.

Представлені результати підтверджують, що до покращень статистичних характеристик МАГФ призвело збільшення значень модуля m. Збільшення початкового числа в регістрах x_0 мало незначний вплив на проходження тестів NIST.

Висновок

Проведене дослідження псевдовипадкових бітових послідовностей МАГФ продемонструвало можливість покращення його статистичних характеристик. При використанні невеликих значень модуля та початкового числа в регістрах генератор не характеризується повною статистичною безпекою, але збільшення цих параметрів призводить до покращення ефективності та якості генератора. Представлені результати підтверджують, що до покращень статистичних характеристик МАГФ призвело збільшення значень модуля m. Збільшення початкового числа в регістрах x_0 мало незначний вплив на проходження тестів NIST. Було встановлено конкретні значення модуля та початкового числа в регістрах, при яких МАГФ успішно пройшов усі тести NIST. Це підтверджує його задовільні статистичні характеристики та високу криптостійкість.

Таким чином, ці генератори можна застосовувати для рішення криптографічних задач, а також використовувати при проєктуванні складних криптографічних систем.

Перелік посилань

1. Burns, P. Lagged, Fibonacci Random Number Generators. [Електронний ресурс] // – Режим доступу: http://lamar.colostate.edu/~grad511/lfg.pdf (09.05.2014).
2. Cybulski, R. Pseudo-random number generator based on linear congruence and delayed Fibonacci method: Pseudo-random number generator based on linear congruence and delayed Fibonacci method. Tech. Sci. 2021, 24, 331–349.
3. Mandal, K.; Fan, X.; Gong, G. Design and implementation of warbler family of lightweight pseudorandom number generators for smart devices. ACM Trans. Embed. Comput. Syst. TECS 2016, 15, 1.
4. Baldoni, S.; Battisti, F.; Carli, M.; Pascucci, F. On the Use of Fibonacci Sequences for Detecting Injection Attacks in Cyber Physical Systems. IEEE Access 2021,9, 41787–41798.
5. Cardell, S.D.; Requena, V.; Fuster-Sabater, A.; Orue, A.B. Randomness Analysis for the Generalized Self-Shrinking Sequences. Symmetry 2019,11, 1460.
6. Murillo-Escobar, M.A.; Cruz-Hernández, C.; Cardoza-Avendaño, L.; Méndez-Ramírez, R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dyn. 2017,87, 407–425.
7. Meranza-Castillón, M.O.; Murillo-Escobar, M.A.; López-Gutiérrez, R.M.; Cruz-Hernández, C. Pseudorandom number generator based on enhanced Hénon map and its implementation. J. AEU-Int. J. Electron. Commun. 2019,107, 239–251.
8. Hamza, R. A novel pseudo random sequence generator for image-cryptographic applications. J. Info. Secur. Appl. 2017,35,119–127.
9. Maksymovych, V.; Mandrona, M.; Harasymchuk, O. Dosimetric Detector Hardware Simulation Model Based on Modified Additive Fibonacci Generator. Adv. Intell. Syst. Comput. 2020, 938, 162–171
10. Maksymovych, V.; Shabatura, M.; Harasymchuk, O.; Karpinski, M.; Jancarczyk, D.; Sawicki, P. Development of Additive Fibonacci Generators with Improved Characteristics for Cybersecurity Needs. Appl. Sci. 2022, 12, 1519.
11. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Електронний ресурс]. – Доступно з: https://csrc.nist.gov/ publications/detail/sp/800-22/rev-1a/final
12. Schneier, B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C. New York, John Wiley & Sons, (1996), 758 p. ISBN-13: 978-0471117094.

Надійшла 04.05.2024