УДК 519.683

С. М. Білан, к.т.н., професор
(професор кафедри «Телекомунікаційні технології та автоматика» Державного економіко-технологічного університету транспорту)
О. І. Левчук
(курсант с-24 взводу, С 2 курсу, Інститут спеціального зв'язку та захисту інформації, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»)

ДОСЛІДЖЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ АСИНХРОННОГО КЛІТИННОГО АВТОМАТУ

В роботі розглядається генератор псевдовипадкових бітових послідовностей, який реалізований на асинхронному клітинному автоматі. Використовується околиця фон Неймана, стан якої указує напрямок передачі активного сигналу. Представлена апаратна реалізація генератора і виконано його програмне моделювання. Проведено тестовий аналіз сформованих бітових послідовностей.

Ключові слова: *генератор псевдовипадкової послідовності чисел, клітинний автомат.*

В работе рассматривается генератор псевдослучайных битовых последовательностей, который реализован на асинхронном клеточном автомате. Используется окрестность фон Неймана, состояние которой указывает направление передачи активного сигнала. Представлена аппаратная реализация генератора и выполнено его программное моделирование. Проведено тестовый анализ сформированных битовых последовательностей.

Ключевые слова: *генератор псевдослучайной последовательности чисел, клеточный автомат.*

Вступ. На сьогодні існує велика кількість генераторів псевдовипадкових чисел, які ефективно використовуються у різних галузях людської діяльності [1-8]. Реалізація генераторів має різну природу. Велика кількість розроблених генераторів псевдовипадкових чисел (ГПВЧ) обумовлена широким їх застосуванням в різних областях людської діяльності. Особливу необхідність застосування ГПВЧ мають такі області як: криптографія, захист і діагностика систем передачі даних, теорія ігор, імітаційне моделювання та у багатьох інших областях. Всі кошти і процеси, в яких використовуються ГПВЧ, можна розділити на використання отриманої послідовності випадкових чисел, як в статиці, так і в динаміці. Використання статичної послідовності випадкових чисел є попередньою генерацією випадкових чисел і формування бази даних. Потім згенерована послідовність ефективно використовується. Існує також необхідність генерації і використання випадкових чисел в реальному масштабі часу.

Однак існуючі запити не завжди задовольняються вже існуючими генераторами. Це обумовлено труднощами досягнення оптимальних значень основних параметрів ГПВЧ. До таких основних параметрів належать:

1. Довжина періоду повторення послідовності випадкових чисел.

2. Низькі статистичні властивості сформованої послідовності.
3. Низька швидкодія.
4. Ступінь незалежності чисел послідовності.
5. Діапазон значень чисел для вибору.

Для кожної задачі можуть бути прийняті до уваги окремі характеристики, які впливають на результат рішення задачі. Вони залежать від структури ГПВЧ та алгоритму генерації бітової послідовності, а також значення має його програмна або апаратна реалізація. Наприклад, апаратна реалізація значно підвищує швидкодію, але такий підхід потребує додаткових витрат ресурсів і спеціалізованої підготовки розробника.

Аналізуючи сучасний стан розвитку ГПВЧ, а також якості їх функціонування, стає зрозумілим, що потреба у створенні та розробці нових джерел генерації псевдовипадкових послідовностей, що поєднують у собі високу швидкодію і хороші статистичні властивості формованої вихідної послідовності, досі залишається актуальною.

Постановка задачі. Завданням даної роботи є створення генератора псевдовипадкових послідовностей чисел, заснованого на клітинному автоматі, який простий у реалізації і володіє високими статистичними характеристиками і високою швидкодією.

ГПВЧ на основі КА. Для побудови ГПВЧ використовується КА. Однак існуючі генератори, побудовані на основі КА, не дають бажаних результатів [5-8]. Наприклад, ГПВЧ на основі одновимірного КА, який розробив Стівен Вольфрам [5, 6], формує цілком випадкову послідовність чисел. Однак застосування такого генератора для шифрування не дало необхідного захисту і може бути розтин шифру при відомому відкритому тексті [2, 3].

Відомі та багато досліджені ГПВЧ, які реалізують різними клітинами декілька різних локальних функцій. Такі КА називають гібридними КА (ГКА) [9]. У таких ГКА реалізуються різні варіанти еволюції КА і формуються різні псевдовипадкові послідовності. Об’єднання правил для різних клітин КА дає псевдовипадкову послідовність чисел. Однак незмінність їх функціонування і при малій загальній кількості клітин призводить до формування повторів значень. Якщо клітин, які реалізують неоднорідні локальні функції, використовується мало для реалізації правила, то бітова послідовність не виглядає як псевдовипадкова. Це доводять різноманітні тести.

Набули популярності такі підходи, які використовують інші окремі ГПВЧ, що реалізують додаткове джерело псевдовипадкової послідовності біт для КА. Фактично вони стають стартовими для роботи КА. Додаткові ГПВЧ, як правило, реалізуються на регістрі зсуву з лінійними зворотними зв’язками [10 – 13].

При всьому цьому збільшується кількість зв’язків для кожної клітини КА, що знижує надійність функціонування. Крім того, збільшення кількості клітин при аналізі спричиняє зниження швидкодії генератора. А використання додаткового генератора для перемішування реалізованого на регістрі зсуву із зворотними зв’язками зазвичай покращує його властивості. Однак це збільшує кількість зворотних зв’язків, що також знижує швидкодію. У запропонованих генераторах використовується неоднорідність, яка вимагає його жорсткої початкової настройки. Це збільшує кількість вихідних установок. Проблемою також є і те, що використання кількох КА і одного регістра зсуву в два рази ускладнює схематичну реалізацію. При цьому не показано, за яким законом здійснюється зміна станів обох КА. Фактично здійснювалося додавання за модулем 2 трьох бітів. Два біта визначаються функціями від масиву клітин, які представляли частина клітин відповідного КА, а третій біт є біт на виході генератора, реалізованого на регістрі зсуву з лінійними зворотними зв’язками. Фактично використовується три окремі генератори, вихідні біти яких є аргументами результуючої функції. Всі генератори псевдовипадкових чисел, заснованих на КА, залежать від поведінки самих КА і від особливостей їх організації.

Модель ГПВП на основі асинхронного КА. ГПВП реалізується двома складовими: самим КА та системою комутації [14]. Клітинний автомат на кожному такті змінює власний стан. Фактично у такому КА власний стан змінює тільки одна клітина, яка називається активною або збудженою. У кожний наступний момент часу активною стає та клітина, на яку указує активна клітина у поточний момент часу. Активною може стати клітина, яка входить до об'єднаної групи клітин по топологічному розташуванні. Як правило використовують клітини, що належать околиці.

Для побудови робочої моделі використовують кодування для клітин околиці (рис. 1).

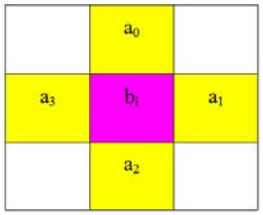

Рис. 1. **Кодування клітин за околицею фон Неймана**

Розглянемо поведінку системи, яка має активний стан. Кожна клітина описується такою моделлю.

$$b_i(t+1)=\begin{cases} f = b_i(t)\oplus a_0(t)\oplus b_1(t)\oplus b_2(t)\oplus b_3(t), & якщо \ \bigvee_{j=0}^{3} C_j(t)=1 \\ b_i(t), & якщо \ \bigvee_{j=0}^{3} C_j(t)=0 \end{cases},$$

де $b_i(t)$ – стан клітини у момент часу t;

$C_j(t)$ – значення сигналу на *j*-му вході активації у момент часу t $j=\overline{0,3}$.

Кількість входів активації у кожної клітини визначається кількістю клітин околиці. Виникає необхідність визначення локальної функції активації, яка указує наступну активну клітину. Для досліджуваного ГПВЧ використовувалась околиця фон Неймана. Тобто кожна клітина мала чотири виходи активації, а отже вона виконує чотири локальних функції активації. Дані локальні функції активації описуються наступними логічними виразами

$$y_0(t+1)=\overline{a_0(t)}\wedge\overline{a_1(t)};$$
$$y_1(t+1)=\overline{a_0(t)}\wedge a_1(t);$$
$$y_2(t+1)=a_0(t)\wedge\overline{a_1(t)};$$
$$y_3(t+1)=a_0(t)\wedge a_1(t).$$

У даному випадку сигнал $y_0(t)$ подається на вхід активації $C_2(t)$ верхньої клітини околиці контрольної клітини. Якщо $y_0(t+1)=C_2(t+1)=1$, то клітина a_0 переходить у активний стан.

Таким чином, кожна клітина клітинного автомату може мати два стани: інформаційний і активний. Інформаційні стани клітин околиці вказують напрямок передачі сигналу збудження.

Програмна реалізація ГПВП на основі асинхронного КА. Згідно з побудованою моделлю розроблена програма, яка моделює процес генерації псевдовипадкової бітової послідовності на основі клітинного автомату. КА реалізований за околицею фон Неймана. Інтерфейс програми демонструє динаміку зміни станів клітинного автомату під час генерації псевдовипадкової бітової послідовності. Початковий інтерфейс програми відкривається шляхом запуску файлу Project1.exe (рис. 2).

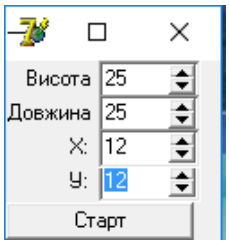

Рис. 2. **Початковий інтерфейс програми «Generator_PVP_L»**

За допомогою початкового інтерфейсу задаються розміри матриці та координати початкової точки. Матриця автоматично заповниться логічними «1» та «0», які вказують початковий стан клітин. Після початкових установок ГПВЧ на екрані відображаються стани КА, поточна активна клітина та її околиця (рис. 3).

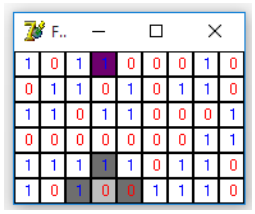

Рис. 3. **Поточний інтерфейс роботи програми «Generator_PVP_L»**

Програма дозволяє зберегти результати у файлі формату «txt». Приклад сформованої бітової послідовності подано на рис. 4.

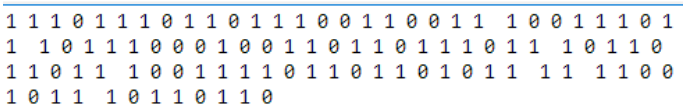

Рис. 4. **Приклад сформованої бітової послідовності**

Оцінка якості сформованих випадкових послідовностей. Є множина тестів для перевірки псевдовипадкових послідовностей, які детально описані в різних літературних джерелах [2, 3]. Усі вони поділяються на графічні і статистичні. Існує програмне забезпечення, яке розміщене на різних сайтах, які дають можливість провести оцінку потрібної послідовності чисел. До таких програм відносять: ENT, DIEHARD, RABENZIX, NIST тощо. Деякі програми оновлюються, і кількість реалізованих тестів у них збільшується. Вважається, що чим більше тестів проведено успішно, тим ближче послідовність до випадкової. Для нашого генератора були використані тести, описані програмою ENT [15]. Дана програма реалізує такі тести:

1. Обчислює ентропію. Тест описаний в роботі [16]. Згідно з цим тестом визначається розмір стиснення отриманого файлу. Послідовність вважається випадковою, якщо стиснення файла не зменшує його розміру.

2. Chi-square Test. Даний тест дозволяє визначити величину відсотка, який вказує частоту перевищення розрахованого значення. Цей відсоток дає оцінку випадковості послідовності [17].

3. Arithmetic Mean. Простий арифметичний тест, який визначає величину, отриману в результаті розподілу суми байтів на довжину файла. Для випадкової послідовності величина має бути близькою до 0,5.

4. Monte Carlo Value for Pi. Тест визначає відсоток влучень значень в коло, вписане в квадрат. Обчислюється число Pi. Якщо це число наближається до значення 3,143580574, то послідовність визначається як випадкова.

5. Serial Correlation Coefficient. Тест визначає залежність кожного байта від попереднього. Для випадкових послідовностей ця величина прагне до 0 [17].

Для тестування було сформовано кілька послідовностей з довжиною 1000, 100000, 500000 і 1000000 біт. Усі тести для всіх послідовностей були успішними і вказали на те, що послідовності можуть вважатись випадковими. У табл. 1 представлені значення основних величин для кожного тесту для вибіркової групи послідовностей.

Таблиця 1. **Результати проведених семи тестів NIST**

Тест	Результат
Частотний тест	Ефективність 91%
Частотний тест по блокам	Значення P(value)=0.262 отже послідовність випадкова
Тест Серій	Значення P(value)=0.42 отже послідовність випадкова
Тест найдовшої серії з одиниць	Значення igamc()=0.14 отже послідовність випадкова
Тест на основі дискретного перетворення Фур'є	Значення P(value)=0.12 отже послідовність випадкова
Тест рангу бінарних матриць	Значення P(value)=0.37 отже послідовність випадкова
Спектральний тест	Значення P(value)=0.29 отже послідовність випадкова

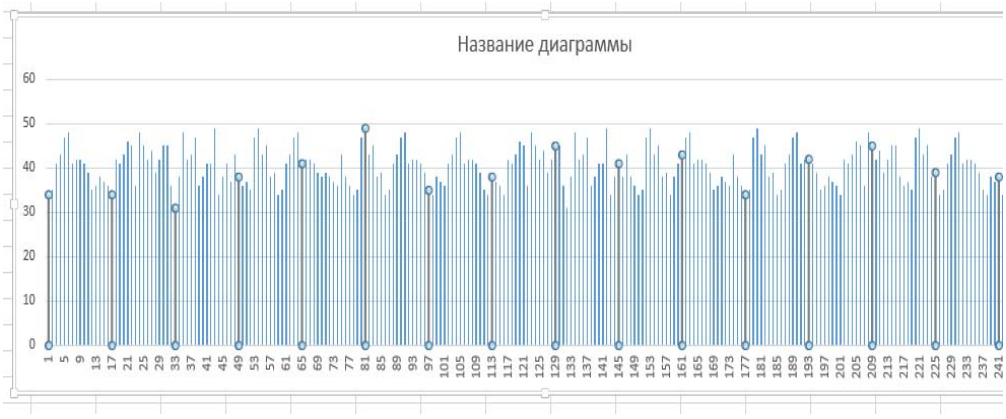

Рис. 5. **Графічний тест роботи генератора**

На рис. 5 показаний результат графічного тесту для 10376 чисел послідовності. Форма графіка дає можливість стверджувати, що результат є непоганим, адже нема таких чисел в діапазоні від 0 до 256, які не попадались. Загальна кількість кожного числа з цього проміжку, яке формувалося генератором, лежала в діапазоні від 34 до 49.

Висновок. У роботі представлені дослідження генератора псевдовипадкових послідовностей чисел, заснований на асинхронному КА. У даному генераторі використовується локальна функція передачі активного стану, яка дає псевдовипадкову бітo-

ву послідовність з високими статистичними властивостями. Дана функція має два аргументи, які подаються станами перших двох клітин околиці. Генератор також має високу швидкодію при його апаратній реалізації. У запропонованому генераторі відсутні зворотні зв'язки, що підвищує його надійність функціонування.

Подальші дослідження. Авторами розроблено кілька модифікацій генераторів заснованих на таких КА. Ми плануємо збільшити кількість відомих тестів для якісного аналізу запропонованих генераторів.

ЛІТЕРАТУРА

1. Брюс Шнайер.. «Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. 2-е издание». – М.: Дело, 2003. – 524 с.

2. *Чугунков И.В.* Методы и средства оценки качества генераторов псевдослучайных последовательностей, ориентированных на решение задач защиты информации: Учебное пособие. М.: НИЯУ МИФИ, 2012 – 236 с.

3. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

4. *von Neumann J.* Various techniques used in connection with random digits // Applied Mathematics Series. Vol, 1951. – № 12. – P. 36–38.

5. *L'Ecuyer P.* Uniform random number generation // Annals of Operations Research. Vol, 1994. – № 53. – P. 77–120.

6. Wolfram S. Random sequence generation by cellular automataю- Advances in Applied Mathematics. – 1986. – Vol. 7. – P. 123–169.

7. *Lehmer D.* Mathematical methods in large-scale computing units //Large-Scale Digital Calculating Machinery: Symp. proc. Harvard, 1951. – P. 141–146.

8. Thomson W. A modified congruence method of generating pseudo-random numbers // Computer Journal. Vol, 1958. –P. 83-86.

9. Cho S. J. New syntheesis of one-dimensional 90/150 liner hybrid group CA / S. J. Cho, U. S. Choi, H. D. Kim, Y. H. Hwang, J. G. Kim, S. H. Heo // IEEE Transactions on comput-aided design of integrated circuits and systems, 2007. – No. 25 (9). – P. 1720–1724.

10. *Marsaglia G.* Random number generators // Journal of Modern Applied Statistical Methods. Vol, 2003. – № 2. – P. 2–13.

11. *Eichenauer J., Lehn J., Topuzoglu A.* A nonlinear congruential pseudorandom number generator with power of two modulus // Mathematics of Computation. Vol, 1988. – 51. – P. 757–759.

12. *Lewis T., Payne W.*. Generalized feedback shift register pseudorandom number algorithms // Journal of ACM. Vol, 1973. – № 21. – P. 456–468.

13. Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов / Б.М. Сухинин // Прикладная дискретная математика, 2010. – № 2. – С. 34 – 41.

14. S. Bilan, M. Bilan, S. Bilan. Novel pseudo-random sequence of numbers generator based cellular automata.- Information Technology and Security. January-June 2015. Vol. 3. Iss. 1 (4).- P. 38–50.

15. http://www.fourmilab.ch/random/

16. Hamming, Richard W. Coding and Information Theory. *Englewood Cliffs NJ: Prentice-Hall, 1980.*

17. *Knuth, Donald E.* The Art of Computer Programming, Volume 2 / Seminumerical Algorithms. Reading MA: Addison-Wesley, 1969.

Stepan M. Bilan, PhD (Technical Sciences), Professor
(Professor Telecommunication Technology and Automation Chair, State University for Transport Economy and Technologies)
Oleg Levchuk
(Cadet of the** Institute of Special Communication and Information Protection **National Technical University of Ukraine «Igor Sikorsky Kyiv polytechnic institute»)

RESEARCH PSEUDORANDOM NUMBER GENERATOR BASED ON ASYNCHRONOUS CELLULAR AUTOMATON

The pseudorandom bit sequence generator that is implemented on asynchronous cellular automata is considered. The neighborhood von Neumann, the state of which indicates the direction of transfer of the active signal is used. The generator hardware implementation and software modeling are presented. A test analysis generated bit sequences was carred out. In the paper is presented the results test in the form of a chart that shows quite a good bit sequence generator that was formed. Designed generator is easy to use and has a high statistical characteristics and high performance. The generator has been designed with two components: by cellular automata and systems of comutation.

Keywords: *generator pseudorandom sequence of numbers, cell makers.*

REFERENCES

1. Bruce Schneier. «Applied cryptography. Protocols, and algorithms for language yshodnue tekstu S. 2nd edition , M .: Case 2003- 524s

2. I.V. Chuhunkov Methods and sredstva otsenki quality generators psevdosluchaynыh sequences, oriented to the decision of problems of protection of information: Uchebnoe posobye. M .: NYYAU MiFi, 2012, 236 p.

3. *Ivanov M.A, Chuhunkov I.V* Application and evaluation of quality generators psevdosluchaynuh posledovatelnostey, N .: KUDYTS images, 2003, 240 p.

4. *von Neumann J.* Various techniques used in connection with random digits [Applied Mathematics Series.] Vol, 1951, 12. P. 36-38.

5. *L'Ecuyer P.* Uniform random number generation [Annals of Operations Research.] Vol, 1994, 53. P. 77-120.

6. Wolfram S. Random sequence generation by cellular automataю- Advances in Applied Mathematics, Vol, 1956 –7, P. 123-169.

7. *Lehmer D.* Mathematical methods in large-scale computing units [Large-Scale Digital Calculating Machinery: Symp. proc. Harvard] 1951, P. 141-146.

8. Thomson W. A modified congruence method of generating pseudo-random numbers [Computer Journal.] Vol, 1958, P. 83-86.

9. Cho S. J. New syntheesis of one-dimensional 90/150 liner hybrid group CA / S. J. Cho, U. S. Choi, H. D. Kim, Y. H. Hwang, J. G. Kim, S. H. Heo [IEEE Transactions on comput-aided design of integrated circuits and systems] 2007, No. 25 (9), P. 1720-1724.

10. *Marsaglia G.* Random number generators [Journal of Modern Applied Statistical Methods.] Vol, 2003 – 2. P. 2-13.

11. *Eichenauer J., Lehn J., Topuzoglu A.* A nonlinear congruential pseudorandom number generator with power of two modulus [Mathematics of Computation.] Vol, 1988 – 51. P. 757-759.

12. *Lewis T., Payne W.*. Generalized feedback shift register pseudorandom number algorithms [Journal of ACM.] Vol, 1973 – 21. P. 456-468.

13. Sukhinin B.M. Vusokoskorostnue generators psevdosluchaynuh sequences based kletochnuh avtomatov / BM Sukhinin [Applied discrete mathematics] 2010, No. 2, P. 34 – 41.

14. S. Bilan, M. Bilan, S. Bilan. Novel pseudo-random sequence of numbers generator based cellular automata.- Information Technology and Security. January-June 2015. Vol. 3. Iss. 1 (4).- p. 38-50.

15. http://www.fourmilab.ch/random/

16. Hamming, Richard W. Coding and Information Theory. *Englewood Cliffs NJ: Prentice-Hall, 1980.*

17. *Knuth, Donald E.* The Art of Computer Programming, Volume 2 [Seminumerical Algorithms. Reading MA: Addison-Wesley], 1969.