PHYSICAL AND TECHNOLOGICAL PROBLEMS OF RADIO ENGINEERING DEVICES, TELECOMMUNICATION, NANO- AND MICROELECTRONICS

PROCEEDINGS

of the IVth International Scientific-Practical Conference

Dedicated to the 25th anniversary from the foundation
of the Department of Radio Engineering Devices and Information Security
Yuriy Fedkovych Chernivtsi National University

October 23-25, 2014, Chernivtsi, Ukraine

ПРИСТРІЙ ГЕНЕРУВАННЯ ХАОТИЧНИХ СИГНАЛІВ НА ОСНОВІ ДИСКРЕТНИХ ОДНОМІРНИХ ВІДОБРАЖЕНЬ

Гресь О.В.[1], Політанський Р.Л.[1], Верига А.Д.[1], Іванчук М.М.[2]
[1]*Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна, E-mail: alexgs85@ukr.net*
[2]*ПП "АРТОН", Чернівці, Україна*

Анотація *– в даній роботі запропонована апаратна реалізація пристрою генерування хаотичних сигналів на основі дискретних одномірних відображень. Результати моделювання пристрою підтверджені результатами експериментальних досліджень.*

Ключові слова: *псевдовипадкова послідовність, генератор, криптостійкість.*

I. Вступ

Сучасні телекомунікаційні системи вимагають забезпечення високої скритності і конфіденційності зв'язку. Захист інформації в даних системах можливий шляхом її шифрування інформації за допомогою хаотичних послідовностей. Це сприяло розробці принципово нових методів кодування, шифрування та передавання інформації, зокрема криптографічних методів, що ґрунтуються на теорії динамічних систем з притаманними їм властивостями хаосу. Криптографічні методи захисту інформації залишаються найбільш стійким і захищеним способом передавання даних

В літературних джерелах описано багато методів генерування двійкових псевдо випадкових послідовностей. Одним із найпоширеніших методів є генерування послідовності на основі певного рекурентного співвідношення, що зв'язує цілі або дійсні числа. Тоді черговий біт двійкової послідовності отримують на основі визначення належності члена послідовності до однієї з двох підмножин усіх можливих значень [1].

II. Реалізація пристрою

Практичну реалізацію пристроїв генерування псевдовипадкових послідовностей можна здійснити з використанням сучасної елементної бази (мікроконтролерів, програмованих логічних інтегральних схем та ін.), що забезпечує покращення їх масогабаритних показників, розширення функціональних можливостей та підвищення швидкості обробки даних[2].

В даній роботі запропонована апаратна реалізація пристрою генерування псевдовипадкових послідовностей на основі одномірних дискретних хаотичних відображень. Структурна схема пристрою приведена на рис.1

Основою пристрою є мікроконтролер DD1 (PIC18F252), який виконує функції апаратного програмованого ядра для генерування послідовностей за певним алгоритмом.

Електрична принципова схема пристрою приведена на рис.2.

Рис. 1 Структурна схема пристрою

Для генерування цифрових хаотичних послідовностей використовується одномірне дискретне відображення, що носить назву логістичного рівняння [3]:

$$x_{n+1} = \lambda \cdot x_n \left(1 - x_n\right) \quad (1)$$

де: λ – параметр, x_0 - початкова умова для генерування послідовностей. Генерування хаотичної послідовності у відповідності з цим рівнянням має місце при значеннях параметру $\lambda \in [3{,}65 \div 3{,}95]$. В нашому випадку генерування послідовностей здійснювалось при значенні параметру λ рівному 3,94 та початковій умові x_0 =0,5.

Значення початкової умови x_0 та параметру λ задаються при програмуванні мікроконтролера. Генерування послідовностей здійснюється на програмному рівні. Програма для мікроконтролера написана на мові програмування С.

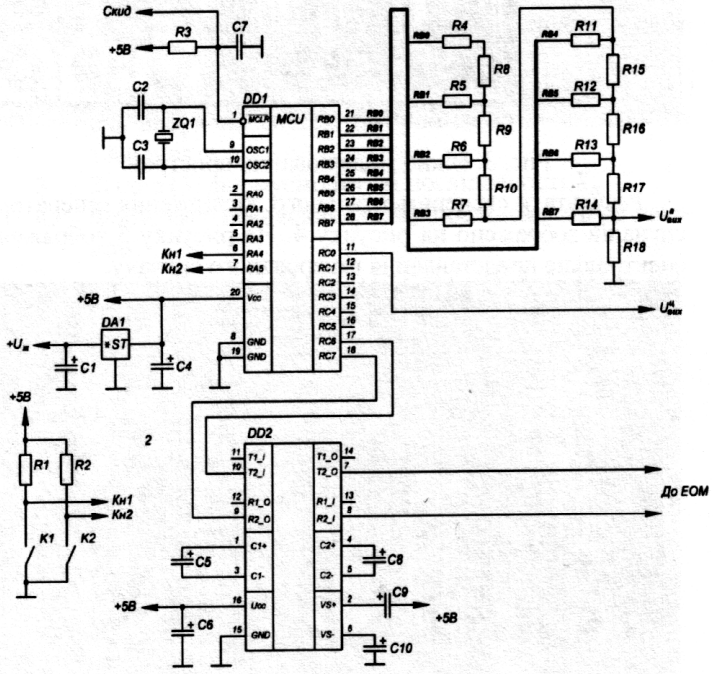

Рис. 2 Електрична принципова схема пристрою

Криптостійкість пристрою обумовлена простором ключів для генерування послідовностей, що є значенням параметра логістичного відображення λ та початкового значення x_0. Обсяг простору ключів буде визначатися за формулою:

$$N = (10^n)^2 \quad (3)$$

де n – точність введенння параметрів (кількість знаків після коми).

Пристрій узгодження інтерфейсу RS-232 виконаний на мікросхемі DD2 (MAX232) та призначений для зв'язку пристрою з ЕОМ для керування (із можливістю завантаження керуючої програми мікроконтролера за допомогою завантажувача „bootloader").

Для живлення схеми використано інтегральний стабілізатор DA1 (LM7805) так як всі використані в приладі мікросхеми та дискретні компоненти живляться однополярною напругою +5В. Режим роботи пристрою можна вибрати за

допомогою пари перемикачів K1,K2. Пристрій може працювати в одному з трьох режимів

1. Генерування аналогового хаотичного сигналу
2. Формування цифрового послідовного коду
3. Робота з ЕОМ, із можливістю передачі коду через інтерфейс RS-232.

Моделювання роботи пристрою було здійснено в програмному середовищі Proteus. Результати приведені на рис.3.

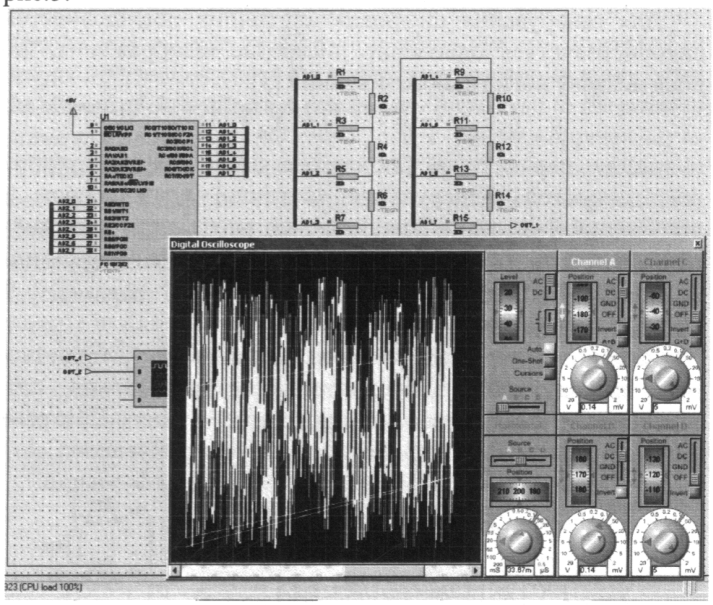

Рис. 3. Вікно моделювання пристрою

Результати експериментального дослідження генератора сигналів зображено на рисунку 4. На рисунку 5 зображене спектральне представлення генерованого сигналу

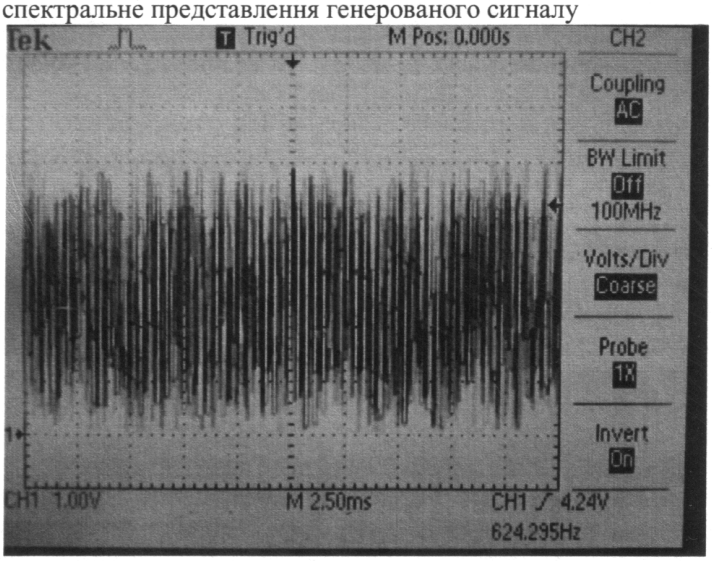

Рис. 4 Вихідний сигнал генератора

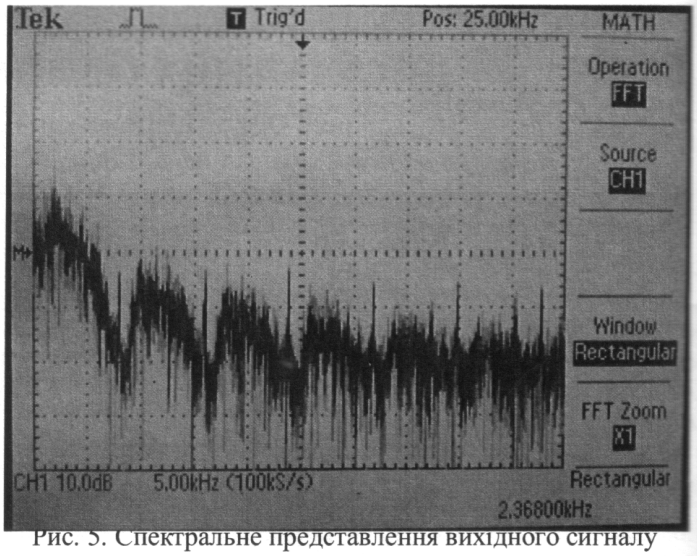

Рис. 5. Спектральне представлення вихідного сигналу

III. Висновки

В даній роботі запропонована апаратна реалізація пристрою генерування хаотичних коливань на основі одномірних дискретних хаотичних відображень. Проведені дослідження пристрою підтвердили можливість застосування мікроконтролерів для генерування хаотичних сигналів із застосуванням сучасних криптостійких алгоритмів.

IV. Список літератури

[1] Kocarev L. Pseudorandom bits generated by chaotic maps / Kocarev L., Jakimoski G. // Circuits and Systems I: Fundamental Theory and Applications, IEEETransactions – 50(1) – 2003 – Pp. 123-126.

[2] Mao Y. A Chip Performing Chaotic Stream Encryption/ Mao Y., Liu W., Li Z., Li P., Halang A. // Studies in Computational Intelligence (SCI) – 42 – 2007 – Pp.307–332.

[3] Pareek N.K. Cryptography using multiple one-dimensional chaotic maps / N.K. Pareek, Vinod Patidar, K.K. Sud // Commun. Nonlinear Sci. Numer. Simul – 10(7) – 2005 – Pp.715–723.

THE DEVICE FOR GENERATING CHAOTIC SIGNALS BASED ON THE ONE-DIMENSIONAL DISCRETE MAPPINGS

Hres O.V.[1], Veryga A.D.[1]., Politans'kyy R.L.[1], Ivanchuk M.M.[2]

[1]Department of the Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

[2]"ARTON", Chernivtsi, Ukraine.

The practical realization of devices for generating pseudo-random sequences can be accomplished using the current base (microcontrollers, programmable logic device, etc..) That provides an improvement in their overall dimensions, enhanced functionality and increased data rate.

In this paper the proposed a hardware implementation of device for generating random signals from one-dimensional discrete chaotic maps. Past studies have confirmed the applicability of the device microcontroller for generating chaotic signals with modern reliability algorithms.