Security of Infocommunication Systems and Internet of Things

2023 Vol 1, No 1

https://doi.org/10.31861/sisiot2023.1.01012

Received 16 June 2023; revised 22 June 2023; accepted 30 June 2023; published 30 June 2023

Using PIC18 Microcontrollers to Generate Chaotic Signals Based on Logistic Mapping

Oleksandr Hres*, Andrii Veryha and Halyna Lastivka

Department of Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine

*Corresponding author (E-mail: o.hres@chnu.edu.ua)

ABSTRACT In this paper, simulation and hardware implementation of the device for generating chaotic signals based on logistic mapping using microcontrollers of the PIC18 series was carried out. The operation of the device was investigated in the mode of generating chaotic oscillations at different values of the control parameter λ. By certain hardware and software modification, this generator can be used as a voice signal encryption The results of simulation and experimental studies confirm the possibility of using PIC18 microcontrollers for the implementation of chaotic oscillation generators based on discrete mappings, as well as using these controllers in the hardware implementation of language information encryption devices.

KEYWORDS generator, logistic mapping, PIC18 microcontroller, scrambler, language information, signal, spectral representation.

I. INTRODUCTION

At present, modern information and telecommunication systems, due to large volumes of circulating information, require high reliability and communication security. Ensuring the protection of transmitted information in these systems is possible by encrypting information using pseudorandom sequences. Currently, there are many algorithms for generating crypto-resistant pseudorandom sequences (PRS), in particular: based on elliptic curves, cellular automata, deterministic chaos theory [1-3]. The main feature of chaotic signal generators, which are implemented on the basis of chaos theory, namely discrete mappings, is high sensitivity to changes in initial conditions [1-3].

II. STUDY OF SOURCES OF CHAOTIC OSCILLATIONS IN DISCRETE SYSTEMS

In some methods of encryption and information protection, chaotic or pseudorandom sequences (PRS) can be used as key sequences or hamming sequences, whose generation algorithms are implemented on the basis of chaos theory, in particular, discrete mappings [1-4]. One of the simplest discrete mappings used to generate sequences is a one-dimensional discrete mapping called the logistic equation, which is described by the following formula [3-5].

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

where: λ is control parameter, x_0 is the initial condition for generating sequences, $x_0 \in (0;1)$.

Depending on the value of λ, the generated oscillations can be periodic, quasi-periodic or chaotic [3]. It was established that for the logistic mapping at $\lambda \geq 3.56$ a mode of chaotic oscillations is observed.

From the bifurcation diagram (FIG. 1) of the logistic mapping it can be seen that at $\lambda \geq 3{,}56$ the period doubling bifurcation has a high frequency, which indicates the chaotic nature of the oscillations [3].

The results of studies of the statistical characteristics of the generator based on the logistic mapping using the NIST STS 2.1.2 test package have shown that the sequences generated on the basis of the logistic mapping have satisfactory statistical characteristics in the range of values of the control parameter $\lambda \in [3{,}8 - 4]$ (array for research was 10^9 bits).

Another key feature of this generator, which provides a large array of generated output sequences, and, accordingly, the stability of the generator, is high sensitivity to changes in the initial parameters (in this case of the accuracy of entering the values of the initial condition x_0 and control parameter λ).

III. SIMULATION OF THE OPERATION OF THE GENERATOR OF CHAOTIC OSCILLATIONS

We will simulate the generator of chaotic oscillations based on the logistic mapping in the LabView 2010 environment with different values of the initial condition X and the control parameter $\lambda \in [3{,}7 - 4]$. The simulation results are shown in FIG. 2.

The simulation results showed that when the control parameter λ increases, the oscillation period doubles. At values of λ from 3.57 and more (Fig. 2 a, b), chaotic behaviour begins, and the doubling cascade ends [4-7]. Small changes in the values of the initial condition or the control parameter lead to large differences in the behaviour of the system over time, which is the main characteristic of chaotic behaviour [4-7].

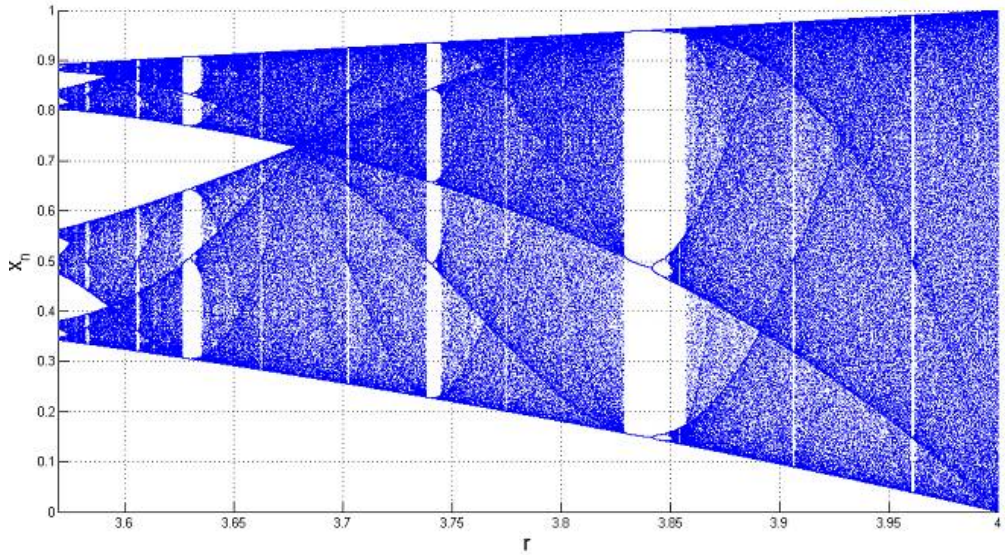


FIG. 1. Bifurcation diagram for logistic mapping for values of $\lambda \in [3,56;4]$.

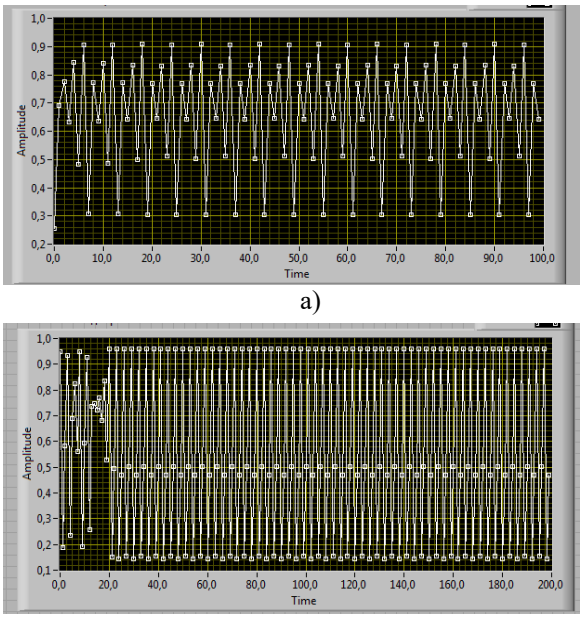


FIG. 2. System simulation at different values of parameter λ: a) λ=3.75; b) λ=3.94.

IV. HARDWARE IMPLEMENTATION OF THE GENERATOR OF CHAOTIC OSCILLATIONS ON A MICROCONTROLLER

We will conduct a study of the possibility of using PIC18 microcontrollers for the hardware implementation and based on discrete mappings. The use of a modern data base (microcontrollers, FPGAs, etc.), provides an improvement in the weight and size indicators of devices, an expansion of the functionality of such devices and an increase in the speed of data processing [4,7,8,9].

This paper proposes a hardware implementation of a chaotic signal generator based on logistic mapping using a PIC18F2550 microcontroller, as well as the possibility of implementing devices for encrypting speech information on their basis.

Structural diagram of the developed generator is given in FIG. 3.

The basis of the device is a DD1 PIC18F2550 microcontroller with a built-in 10-bit ADC, which performs the functions of a hardware programmable core for generating sequences according to a certain algorithm.

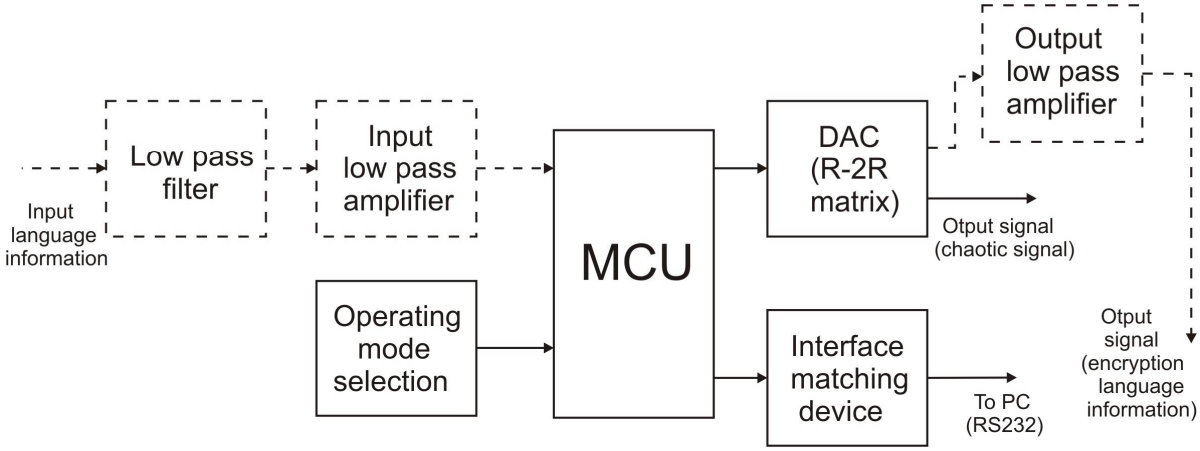


FIG. 3. Structural diagram of the generator of chaotic signals.

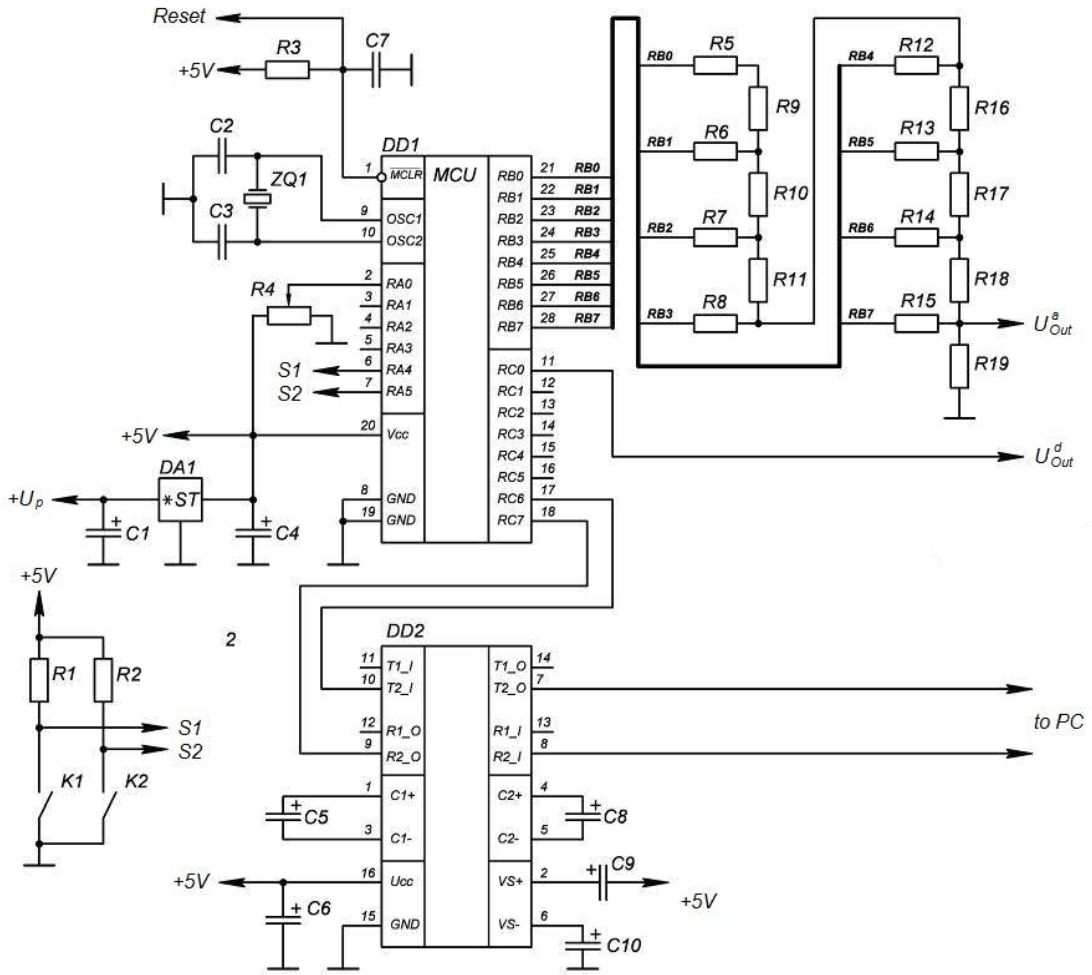


FIG. 4. Electrical schematic diagram of the generator of chaotic signals.

Electrical schematic diagram of the generator is given in FIG. 4.

To generate chaotic signals, the logistic mapping (1) is used with the values of the control parameter $\lambda \in [3.56 \div 4]$ [1-6]. As an algorithm for generating signals, another type of discrete mapping, such as a display awning or the like, can also be used.

The crypto resistance of the device is determined by the key space for generating sequences, which is the value of the logistic mapping parameter λ and the value of the initial condition x_0. The volume of the key space will be determined by the formula [4] :

$$N = (10^n)^2 \qquad (2)$$

where *n* is the accuracy of entering the control parameters and the initial condition (number of decimal places).

The values of the initial condition x_0 and the parameter λ are set when programming the microcontroller. The generation of a chaotic signal based on a given equation is carried out at the software level. The program for the microcontroller is written in the C programming language. The algorithm of the program is shown in the Figure. In FIG.5, the dashed line shows the possibility of modifying the firmware of the microcontroller to implement the speech information encryption device (according to the diagram in FIG.3.)

The device (unit) for matching interfaces is made on a DD2 chip (MAX232) and is intended for communication of the device with a computer via the RS232 port) for control (with the possibility of loading the control program of the microcontroller using the "bootloader").

The generator and all its components are powered by a voltage of +5V, so the integrated stabilizer DA1 (LM7805) is used in the circuit to obtain a stable supply voltage. The operating mode of the device can be selected using a pair of switches K1, K2. The device can work in one of the following modes:

1. Generator mode. In this mode, an analogue chaotic signal (U^a_{out}) is generated according to the programmed generation algorithm. The required value of the control parameter λ (in the range $\lambda \in [3.56 \div 4]$) for generating signals is set by the variable resistor R4. It is also possible to generate a digital serial code (digitized signal) (U^d_{out}).

2. PC connection mode, with the possibility of programming and code transmission through the RS-232 interface.

Simulation of the operation of the proposed generator was carried out in the Proteus 7.2 software environment. The results of simulating the operation of the generator at the value of the control parameter λ = 3.97 are shown in FIG.6.

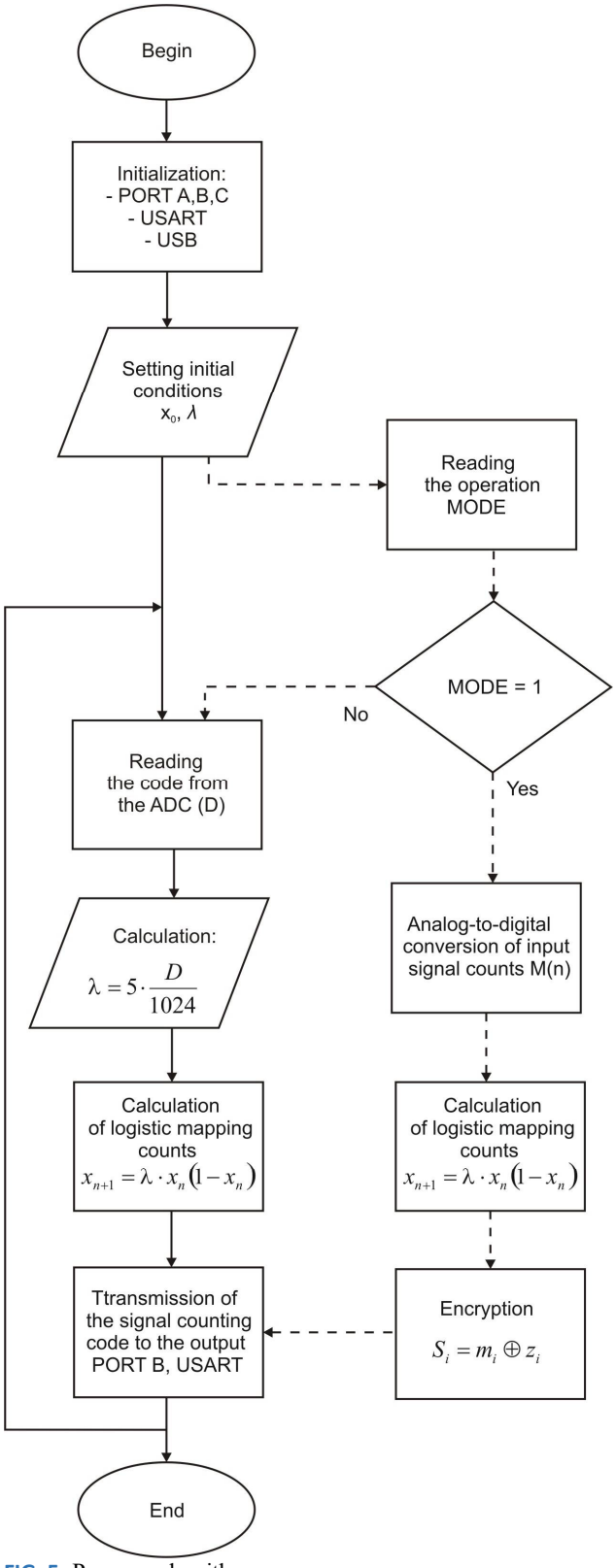


FIG. 5. Program algorithm.

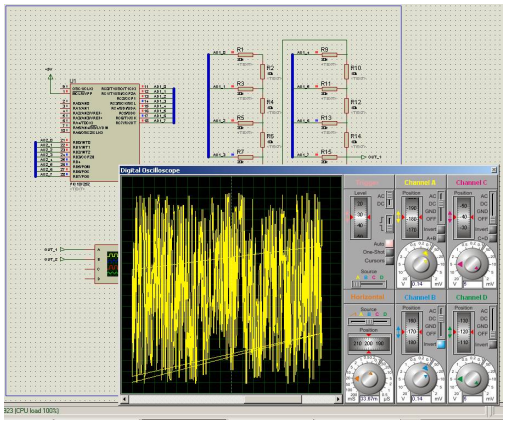
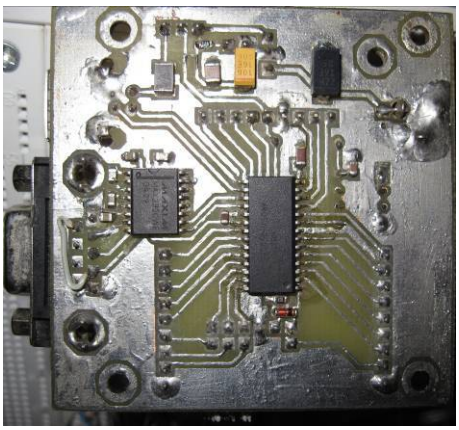
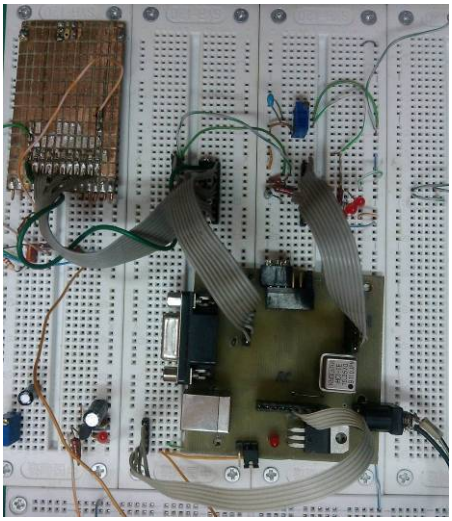


FIG. 6. An example of generator simulation in the Proteus 7.2 environment.

The test version of the device was assembled on a breadboard. The appearance of the layout of the developed signal generator is shown in FIG.7.



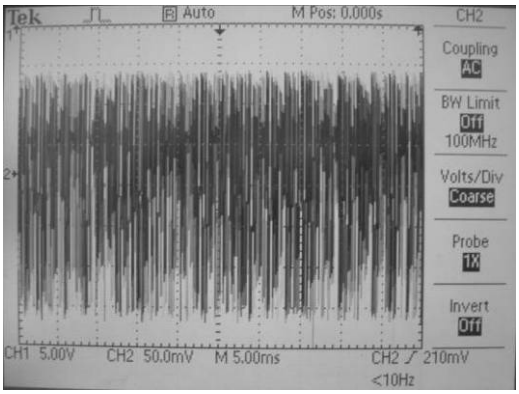
a)



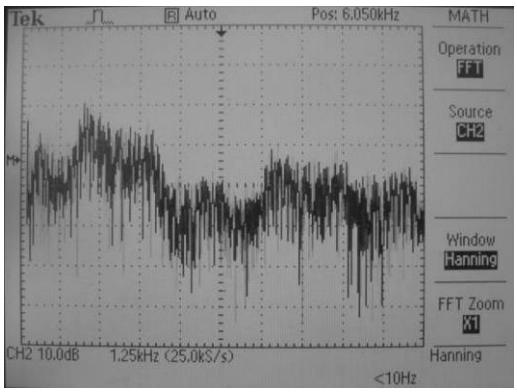
b)

FIG. 7. Appearance a), b) of the generator layout.

The output signals of the generator were studied in the mode of generating an analog chaotic signal at the output of the DAC (R-2R matrix) using a Tektronix TDS1012 digital oscilloscope at different values of the control parameter λ. FIG. 8 and FIG.9 show the signals generated at the values of the control parameter λ = 3.84 and λ = 3.97 (chaotic mode) and their corresponding spectral representation.

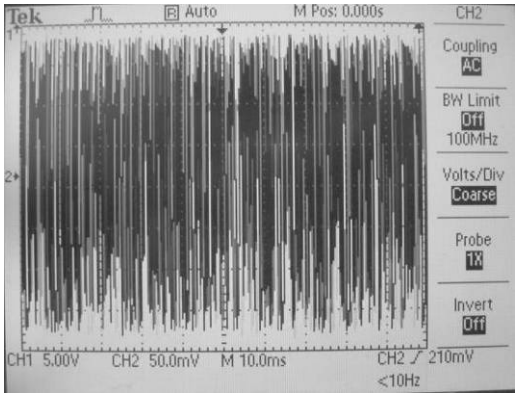


a)

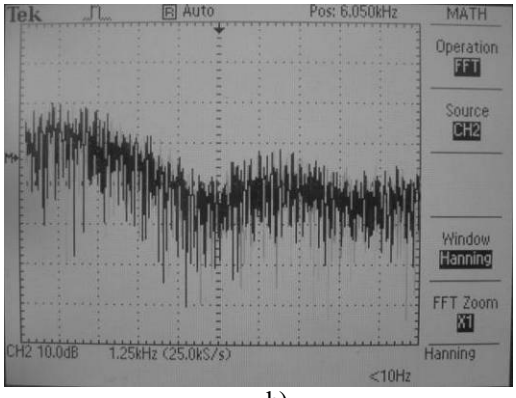


b)

FIG. 8. View a) and spectral representation of the generated signal b) at the value of control parameter λ = 3.84.



a)



b)

FIG. 9. View a) and spectral representation of the generated signal b) at the value of control parameter λ = 3.97.

From the experimentally obtained generated signals and their spectrograms (FIG.8 and FIG.9), it can be concluded that the results of simulating the operation of the generator are confirmed by experimental studies, and, therefore, this generator can be used for the development of crypto-resistant information transmission systems as a source of masking signals.

V. IMPLEMENTATION OF LANGUAGE INFORMATION ENCRYPTION DEVICES

Also, through certain hardware modification and software modification, this generator can be used for the development of speech signal encryptors and for the practical implementation of scramblers [8-12].

Encryptor mode. This mode can be provided by adding the appropriate elements (or units) to the circuit and modifying the firmware of the microcontroller (in FIG.3 and FIG.5 the corresponding elements are marked with a dotted line). In this mode, language information is processed using a microcontroller.

The filtered speech signal from the microphone is amplified and fed to the ADC input of the microcontroller, which digitizes it with a sampling frequency of 8 kHz.

The digitized speech information m_i is added modulo 2 to the chaotic sequence p_i generated on the basis of logistic mapping, forming an encrypted sequence (encrypted speech information) s_i:

$$s_i = m_i \oplus p_i \tag{3}$$

At the same time, the device can also work in decryption mode (on the receiving side).

The process of deciphering information takes place in the reverse order by adding modulo 2 encrypted speech information to the elements of a chaotic sequence, which are generated on the receiving side using a similar logistic equation with the same values of the initial condition X and the control parameter λ.

After decoding, the received language information is transmitted to an external DAC, consisting of an R-2R matrix and the keys of the output port of the microcontroller. From the DAC output, the analog signal is transmitted through the low pass filter and the output low frequency amplifier to the audio output.

FIG. 10 and FIG. 11 show the results of the modified signal generator operation (in the speech information encryptor mode).

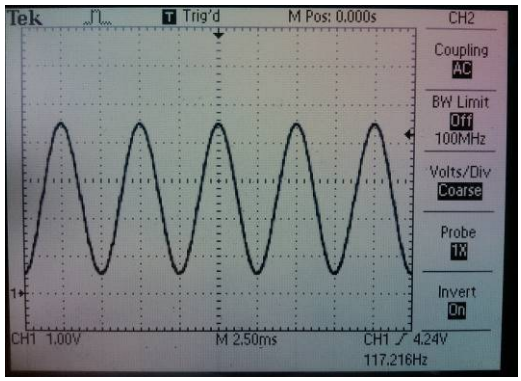
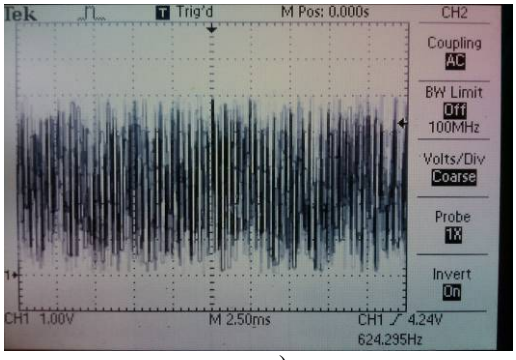
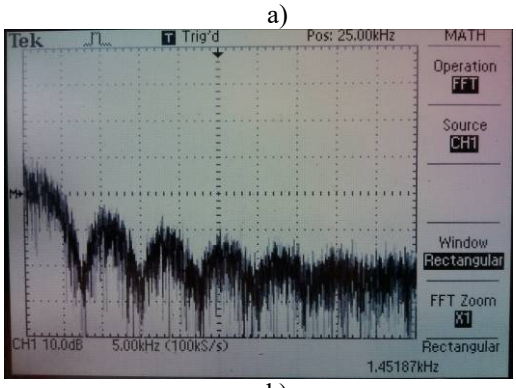


FIG. 10. Input information signal.



a)



b)

FIG. 11. Appearance a) and spectral representation b) of the encrypted speech signal at the value of the control parameter λ = 3.97.

The conducted studies of the device confirmed the possibility of using the PIC18F2550 microcontroller for use in devices for generating chaotic signals and encrypting speech information with the aid of modern crypto-resistant algorithms.

Communication systems developed with the use of such a generator will have sufficient crypto resistance, which is ensured by the presence of a large number of keys (accuracy of entering the initial condition X and the control parameter λ) for generating chaotic sequences.

VI. CONCLUSION

In this paper, simulation and hardware implementation of the device for generating chaotic signals based on logistic mapping using microcontrollers of the PIC18 series was carried out. The operation of the device was investigated in the mode of generating chaotic oscillations at different values of the control parameter λ. By certain hardware and software modification, this generator can be used as a voice signal encryption device. The obtained results of simulation and experimental studies confirm the possibility of using the PIC18F2550 microcontroller for the hardware implementation of generators of chaotic oscillations and devices for encrypting speech information based on discrete mappings. The proposed device can be used both separately for signal generation and for hardware implementation of speech signal encryption devices, scramblers and crypto-resistant information transmission systems based on chaos.

AUTHOR CONTRIBUTIONS

O.H., A.V. – development of the scheme, firmware, implementation of the device; O.H., A.V. – investigation; A.V., H.L. – writing (original draft preparation), H.L. – writing and editing.

COMPETING INTERESTS

The authors declare no competing interests.

REFERENCES

[1] L. Kocarev, G. Jakimoski, "Pseudorandom bits generated by chaotic maps," *Fundamental Theory and Applications, IEEETransactions*, vol.50(1), pp. 123-126, 2003.

[2] Yu. Stasiev, K. Vasiuta, S. Zhenzhera "Informatsiini systemy na osnovi dynamichnoho khaosu," *Systemy ozbroiennia i viiskova tekhnika*, Vol. 1, No 17, s. 134-138, 2009.

[3] L. Acho, "Chaotic logistic map implementation in the PIC12F629 microcontroller," in: *10th International IFAC Workshop on Programmable Devices and Embedded Systems*, Poland, 2010, vol.50, issue 1, pp.167-170.

[4] O. Hres, R. Politanskyi, A. Veryha, M. Ivanchuk, "Prystrii heneruvannia khaotychnykh syhnaliv na osnovi dyskretnykh odnomirnykh vidobrazhen," in *Conf. IV Mizhnarodnoi naukovo-praktychnoi konferentsii Fizyko-tekhnolohichni problemy radiotekhnichnykh prystroiv, zasobiv telekomunikatsii, nano- ta mikroelektroniky*, Chernivtsi, 2014, ss. 83-84.

[5] N. Pareek, V. Patidar, K.Sud, "Cryptography using multiple one-dimensional chaotic maps," *Commun. Nonlinear Sci. Numer. Simu,* vol.10(7), pp.715–723, 2005.

[6] A. Díaz-Méndez, J.V. Marquina-Pérez, M. Cruz-Irisson, R. Vázquez-Medina, J.L. Del-Río-Correa, "Chaotic noise MOS generator based on logistic map," *Microelectron. J.,* vol. 40, pp.638–640, 2009.

[7] Y. Mao, W. Liu, Z. Li, P. Li, A. Halang, "A Chip Performing Chaotic Stream Encryption," *Studies in Computational Intelligence (SCI),* vol. 42, pp.307–332, 2007.

[8] O.V. Hres, A.D. Veryha, R.L. Politanskyi, O.V. Drobyk, "Aparatna realizatsiia prystroiu shyfruvannia movnoi informatsii," *Suchasnyi zakhyst informatsii,* No.3, ss.71-77, 2014.

[9] A-K. Maysa, A-J. Iman Qays, "Speech Encryption Using Chaotic Map and Blowfish Algorithms", *Journal of Basrah Researches (Sciences),* Vol.(39), No.(2), pp. 68-76, 2013.

[10] C. Cruz-Hernández, E. Inzunza-González, R. López-Gutiérrez, H. Serrano-Guerrero, E. García-Guerrero, "Encrypted audio communication based on synchronized unified chaotic systems", *World Academy of Science, Engineering & Technology,* vol.42, pp.475-480, 2010.

[11] A.G. Radwan, "On some generalized discrete logistic maps," *Cairo Univ.: J. Adv. Res*., vol. 4, pp.163–171, 2013.

[12] W.T. Gibson, W.C. Wilson, "Individual-based chaos: extensions of the discrete logistic model," J. Theor. Biol., vol.339, pp.84–92, 2013.

Oleksandr Hres

Yuriy Fedkovych Chernivtsi National University Department of Radio Engineering and Information Security. Ph.D. (Engineering Sciences) Assistant Professor of Department of Radio Engineering and Information Security. Research interests: pseudorandom sequence generators; encryption information, cybersecurity. Author of nearly 42 publications.

Andrii Veryha

Received BS and MS degrees in Radio Engineering from Yuriy Fedkovych Chernivtsi National University, Ukraine. He received a Ph.D. in Radio Engineering from Yuriy Fedkovych Chernivtsi National University. He is currently an assistant of the Radio Engineering Department of Yuriy Fedkovych Chernivtsi National University. His research interests include signal processing, development of electronic circuits.

Halyna Lastivka

Received BS and MS degrees in Radio Engineering from Yuriy Fedkovych Chernivtsi National University, Ukraine; Ph.D. She is currently an associate professor of the Radio Engineering Department of Yuriy Fedkovych Chernivtsi National University. Her research interests include methods and means of radio spectroscopy, their application for research of sensory properties, cybersecurity.

Використання мікроконтролерів типу PIC18 для генерування хаотичних сигналів на основі логістичного відображення

Олександр Гресь*, Андрій Верига та Галина Ластівка

Кафедра радіотехніки та інформаційної безпеки, Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна

*Автор-кореспондент (Електронна адреса: o.hres@chnu.edu.ua)

АНОТАЦІЯ В даній роботі проведене моделювання та апаратна реалізація пристрою генерування хаотичних сигналів на основі логістичного відображення із використанням мікроконтролерів серії PIC18. Моделювання генератора хаотичних коливань на основі логістичного відображення проводилось в середовищі LabView 2010 при різних значеннях початкової умови x_0 та параметру керування $\lambda \in [3{,}7 - 4]$. Роботу пристрою досліджено в режимі генерування хаотичних коливань при різних значеннях параметру керування λ. Результати моделювання показали, що при збільшенні параметру керування λ відбувається подвоєння періоду коливань, а при значеннях λ від 3,7 і більше починається хаотична поведінка, а каскад подвоєнь закінчується. Отже невеликі зміни в значеннях початкової умови або параметру керування призводять до великих відмінностей поведінки системи в часі, що є основною характеристикою хаотичної поведінки. В роботі запропоновано також апаратну реалізацію генератора хаотичних сигналів на основі логістичного відображення з використанням мікроконтролера PIC18F2550, приведені схема електрична структурна, електрична принципова, алгоритм роботи програмного забезпечення та тестовий варіант пристрою на макетній платі. Шляхом певної модифікації апаратного та програмного забезпечення даний генератор може бути використаний в якості пристрою шифрування мовних сигналів. Отримані результати моделювання та експериментальних досліджень підтверджують можливість використання мікроконтролера PIC18F2550 для апаратної реалізації генераторів хаотичних коливань та пристроїв шифрування мовної інформації на основі дискретних відображень. Запропонований пристрій можна використовувати як окремо для генерування сигналів так і для апаратної реалізації пристроїв шифрування мовних сигналів, скремблерів та криптостійких систем передавання інформації на основі хаосу.

КЛЮЧОВІ СЛОВА генератор, логістичне відображення, мікроконтроллер PIC18, шифратор, мовна інформація, сигнал, спектральне представлення.