УДК 004.056.55:004.421.5 https://doi.org/ 10.35546/kntu2078-4481.2019.3.16

T.A. LEVITSKAYA
Pryazovskyi State Technical University, Mariupol
ORCID: 0000-0003-3359-1313
A.V. YABLOKOVA
Pryazovskyi State Technical University, Mariupol
ORCID: 0000-0002-4322-9994

A CRYPTOSYSTEM BASED ON A MATHEMATICAL MODEL OF CHAOTIC OSCILLATIONS GENERATED ON THE BASIS OF DIFFERENTIAL EQUATIONS

At the present time, when widespread and easily accessible technical means are used for the transmission and storage of any data, the protection of information from violations of its confidentiality, integrity, and accessibility is one of the most important problems. The transmitted data can be influenced by the transmission environment or external (information system) environment, as well as various actions of attackers aimed at interception, damage to information. Encryption of transmitted data is one of the methods of protection against malicious attacks. This article is devoted to justification of the use of cryptosystems based on mathematical model of the chaos generator, proposed by Leon Chua in 1983, describing the principles of implementing cryptoalgorithm and prospects of its application. Chaos generator cryptosystems have a number of advantages over symmetric systems and public key systems (the latter are usually used in the form of hybrid cryptosystems when encrypting information), the main problem of which is the length of the key, and as a result - its repeatability. The length of the key obtained from the chaos generator is practically unlimited and each generator can create different processes, which, with a slight change in the initial conditions, make it difficult to determine the structure of the generator. There were described the problems of traditional cryptosystems, the theory of cryptostability, absolutely and computationally stable ciphers, a separate theoretical method for solving the problem of increasing the cryptostability of hybrid computationally stable systems by including a mathematical model of the chaos generator as a key generator for encrypting the data that is transmitted. The scientific novelty of this study is the developed method of applying the mathematical model of the chaos generator "Chua scheme" as the main component of the hybrid cryptosystem, where the chaos generator is used as a source of public and private keys of the asymmetric encryption algorithm and the key of the symmetric algorithm, which is directly used for data encryption. Recommendations and requirements for the implementation of the cryptosystem on the chaos generator "Chua scheme" are described.

Keywords: chaos generator, mathematical model, Chua circuit, encryption, cryptography, information security, deterministic chaos.

Т.О. ЛЕВИЦЬКА
ДВНЗ «Приазовський державний технічний університет»
м. Маріуполь
ORCID: 0000-0003-3359-1313
А.В. ЯБЛОКОВА
ДВНЗ «Приазовський державний технічний університет»
м. Маріуполь
ORCID: 0000-0002-4322-9994

КРИПТОСИСТЕМА НА ОСНОВІ МАТЕМАТИЧНОЇ МОДЕЛІ З ВИКОРИСТАННЯМ ХАОТИЧНИХ КОЛИВАНЬ ГЕНЕРОВАНИХ НА БАЗІ ДИФЕРЕНЦІЙНИХ РІВНЯНЬ

У нинішній час, коли для передачі і зберігання будь-яких даних використовуються поширені легко доступні технічні засоби, питання захисту інформації від порушення її конфіденційності, цілісності, а також доступності є однією з найважливіших проблем. На передані дані можуть впливати середовище передачі або зовнішнє (щодо інформаційної системи) середовище, а також різні дії зловмисників, націлені на перехоплення, пошкодження інформації. Шифрування переданих даних є одним з методів захисту від атак зловмисників. Дана стаття присвячена обґрунтуванню застосування криптосистеми, заснованої на математичній моделі генератору хаосу, запропонованого Леоном Чуа у 1983 році, опису принципів реалізації криптоалгоритму та перспективам його застосування. Криптосистеми на генераторах хаосу мають ряд переваг над симетричними системами і системами з відкритим ключем (останні при шифруванні інформації зазвичай використовуються в формі гібридних криптосистем), головною проблемою яких є довжина ключа, а в результаті - його повторюваність.

Довжина ключа, отриманого від генератора хаосу, практично не обмежена і кожен генератор може створювати різні процеси, які при незначній зміні початкових умов, ускладнюють визначення структури генератора. Розглянуто проблеми традиційних криптосистем, теорії криптостійкості, абсолютно і обчислювально стійких шифрів, окремий теоретичний метод вирішення питання збільшення криптостійкості гібридних обчислювально стійких систем за допомогою включення в них математичної моделі генератора хаосу в якості генератора ключа для шифрування даних, що передаються. Науковою новизною даного дослідження є розроблений метод застосування математичної моделі генератора хаосу «схема Чуа» в якості основного компонента гібридної криптосистеми, де генератор хаосу застосован як джерело відкритого і закритого ключів асиметричного алгоритму шифрування і ключа симетричного алгоритму, безпосередньо використовується для шифрування даних. Описано рекомендації та вимоги щодо реалізації криптосистеми на генераторі хаосу «схема Чуа».

Ключевые слова: генератор хаоса, математическая модель, схема Чуа, шифрование, криптография, защита информации, детерминированный хаос.

Т.А. ЛЕВИЦКАЯ
ГВУЗ «Приазовский государственный технический университет»
г. Мариуполь
ORCID: 0000-0003-3359-1313
А.В. ЯБЛОКОВА
ГВУЗ «Приазовский государственный технический университет»
г. Мариуполь
ORCID: 0000-0002-4322-9994

КРИПТОСИСТЕМА НА ОСНОВЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ХАОТИЧЕСКИХ КОЛЕБАНИЙ СГЕНЕРИРОВАННЫХ НА БАЗЕ ДИФФЕРЕНЦИАЛЬНЫХ УРАВНЕНИЙ

В нынешнее время, когда для передачи и хранения любых данных используются распространенные и легко доступные технические средства, вопросы защиты информации от нарушения ее конфиденциальности, целостности, а также доступности является одной из важнейших проблем. На переданные данные могут влиять среда передачи или внешнее (информационной системы) среда, а также различные действия злоумышленников, нацелены на перехват, повреждение информации. Шифрование передаваемых данных является одним из методов защиты от атак злоумышленников. Данная статья посвящена обоснованию применения криптосистемы, основанной на математической модели генератора хаоса, предложенного Леоном Чуа в 1983 году, описания принципов реализации криптоалгоритму и перспективам его применения. Криптосистемы на генераторах хаоса имеют ряд преимуществ перед симметричными системами и системами с открытым ключом (последние при шифровании информации обычно используются в форме гибридных криптосистем), главной проблемой которых является длина ключа, а в результате - его повторяемость. Длина ключа, полученного от генератора хаоса, практически не ограничено и каждый генератор может создавать различные процессы, которые при незначительном изменении начальных условий, затрудняют определение структуры генератора. Рассмотрены проблемы традиционных криптосистем, теории криптостойкости, абсолютно и вычислительно стойких шифров, отдельный теоретический метод решения вопроса увеличения криптостойкости гибридных вычислительно стойких систем посредством включения в них математической модели генератора хаоса в качестве генератора ключа для шифрования данных, которые передаются. Научной новизной данного исследования является разработанный метод применения математической модели генератора хаоса «схема Чуа» в качестве основного компонента гибридной криптосистемы, где генератор хаоса застосован как источник открытого и закрытого ключей асимметричного алгоритма шифрования и ключа симметричного алгоритма, непосредственно используется для шифрования данных. Описаны рекомендации и требования по реализации криптосистемы на генераторе хаоса «схема Чуа».

Ключові слова: генератор хаосу, математична модель, схема Чуа, шифрування, криптографія, захист інформації, детермінований хаос.

Problem statement

Protection of information from violation of its confidentiality, integrity, and availability is one of the most important problems of the present time, when technical means are used to transfer any data, which can be exposed to an unauthorized access. Encryption is one of the methods of protecting the transmitted data from attacks and unpredictability of the environment. Data encryption allows to confirm their integrity, ensure confidentiality and availability of information for the final recipient. Modern cryptography is characterized by open encryption algorithms that involve the use of computational tools. There is a key of a certain length in this case and a set of relatively simple transformations, so-called cryptographic primitives, such as bitshift, gaming, etc. However, due to the nature of these cryptosystems, there are a large number of methods to decrypt the information encoded by them.

Analysis of recent research and publications

One of the main problems of traditional cryptosystems is that, eventually, the sequence of operations of encryption of the information flow begins to repeat (the key length is limited), and this leads to the fact that the sequence can be disclosed by a third party, and the flow is decrypted. This disadvantage is deprived of absolutely stable ciphers that satisfy a number of the following requirements [1]:

- a key is generated for each block of encrypted data (each key is used only once);
- the key is statistically reliable (the probabilities of occurrence of each of the possible symbols are equal, the symbols in the key sequence are independent and random);
- the key length is equal to or greater than the length of the encrypted data;
- the original (open) text has some redundancy (which is the criterion for evaluating the correctness of the decryption).

The durability of these systems does not depend on the computational capabilities of the cryptanalyst. However, the practical usage of absolutely stable systems is limited due to the complexity and cost of their implementation, so in cryptographic systems, computationally stable systems are mainly used.

A computing-resistant system is a system that has the potential to crack a cipher, but only with selected parameters and encryption keys. The durability of such systems depends on the computational capabilities of the cryptanalyst. The use of chaos generators, which have complex, unpredictable and highly dependent on the initial parameters behavior, as a component of a computationally stable hybrid cryptosystem can significantly increase the cryptographic stability of the cipher. The idea of using chaos generators in signal transmission is not new. Experiments on encryption and decryption of signals by such methods, conducted in the 90s of the 20th century, showed the prospects, attractiveness and effectiveness of the use of chaotic generators in confidential communication systems [2].

Formulation of the aim of work

Formulation of the aim of work **i**s to justify the creation of a cryptosystem based on a mathematical model of a chaos generator (an electric circuit demonstrating chaotic oscillation modes), proposed by Leon Chua in 1983 [3], and to describe the prospects for its application.

Presentation of the main material

Cryptosystems based on chaos generators have a number of advantages over symmetric systems and public key systems (the latter are used in the form of hybrid cryptosystems when encrypting information), the main problem of which, as mentioned earlier, is the length of the key, and as a result – its repeatability. The length of the key obtained with the help of the chaos generator is practically unlimited, and due to the fact that the same chaotic generator can create completely different processes with a slight change in the initial conditions, it is much more difficult to determine the structure of the generator and predict the process for a long time [4], which allows you to create a hacking-resistant system with a high level of reliability.

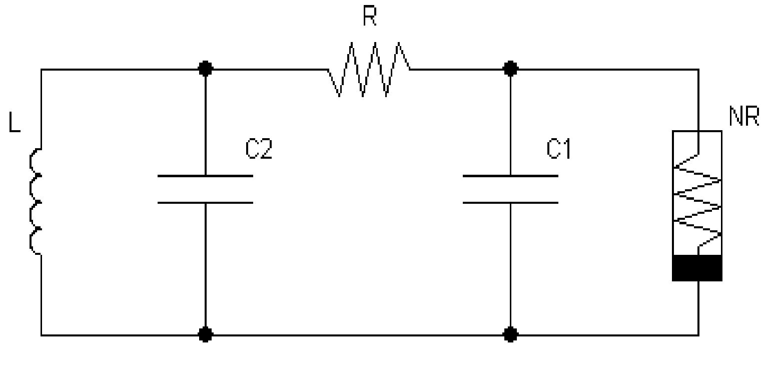

Fig. 1. The Chua Circuit. L, R, C1, and C2 are passive elements, NR is a nonlinear resistor (Chua's diode)

The prospects for the use of chaos generators, in particular the Chua scheme, which will be discussed later, for the protection of transmitted information lies in three features of chaotic processes [4]:

- a chaotic signal has a periodic, continuous spectrum that occupies a sufficiently wide band, and its form can be set;

- the irregularity and unpredictability of the behavior of the chaotic signal, as well as the ability of the chaos generator to create completely different processes with a very slight change in the initial conditions, greatly complicates the prediction of the process for any long time;
- due to the irregularity of chaotic signals, their autocorrelation function quickly fades, which also complicates the prediction of the generation process and the determination of the generator structure.

Due to the fact that the Chua scheme is one of the simplest chaos generators (it is described by only three differential equations and at the same time has a rather complex behavior peculiar to chaos generators), it was chosen for the information encryption system.

As shown in fig. 1, a Chua circuit consists of two capacitors, one inductor, a linear resistor, and a nonlinear negative resistance resistor (commonly called a Chua diode), which in reality can be represented by a circuit complication based on operational amplifiers, inverters, or using a tunnel diode [3].

The Chua scheme is described by the following system of equations [5]:

$$\begin{cases} C_1 \dfrac{dv_{C_1}}{dt} = G\left(v_{C_2} - v_{C_1}\right) - g\left(v_{C_1}\right) \\ C_2 \dfrac{dv_{C_2}}{dt} = G\left(v_{C_1} - v_{C_2}\right) - i_L \\ L\dfrac{di_L}{dt} = -v_{C_2} \end{cases}$$

where $g\left(v_{C_1}\right)$– piece-linear function defined as:

$$g\left(v_{C_1}\right) = G_b v_{C_1} + \frac{1}{2}\left(G_a - G_b\right)\left(\left|v_{C_1} + E\right| - \left|v_{C_1} - E\right|\right)$$

After replacing the coefficients in the system of equations with dimensionless ones, the system will take the following form [5]:

$$\begin{cases} \dfrac{dx}{dt} = a\left(y - x - h(x)\right) \\ \dfrac{dy}{dt} = x - y + z \\ \dfrac{dz}{dt} = -\beta y \end{cases}$$

where $h(x)$ defined as: $g\left(v_{C_1}\right) = G_b v_{C_1} + \frac{1}{2}\left(G_a - G_b\right)\left(\left|v_{C_1} + E\right| - \left|v_{C_1} - E\right|\right)$

The numerical solution of these equations shows that at certain ratios between the components of the chain, the change in the values of variables in time becomes chaotic, a strange attractor of the form "double curl" appears, shown in fig. 2 (the case for the model with dimensionless coefficients) [5].

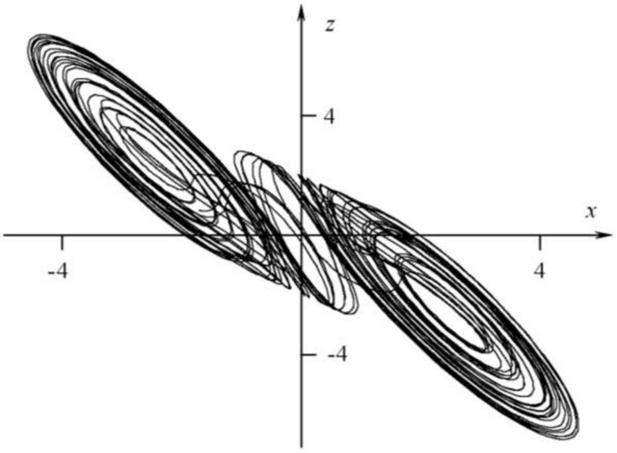

Fig. 2. The Attractor of the “double curl”

The trajectory of such an attractor is non-periodic and the mode of operation is unstable, as a result of which even small deviations of the parameters cause significant changes. The result of this behavior is the nonperiodicity in time of any of the coordinates of the system, the continuous spectrum and the time-decreasing autocorrelation function. This causes the chaotic dynamics of strange attractors, namely, indicates that the prediction of the trajectory that hit the attractor is difficult, since a small inaccuracy in the initial data after some time can lead to a strong discrepancy between the forecast and the real trajectory.

Fig. 3. shows one of the possible time dependences of the change in the value of x for a model with dimensionless coefficients [5].

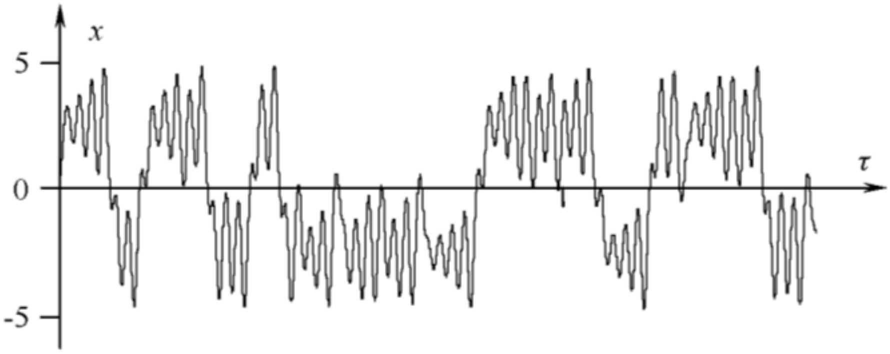

Fig. 3. Time dependence of x change

The time dependence of the change x is one of the parameters that can be used in the cryptosystem to encrypt the transmitted information, for example, by imposing a chaotic signal on the information gamming. In General, encryption can be performed using several algorithms [2]:

- chaotic masking-the information signal is summed with the chaotic signal;
- mode switching-the logical zero is encoded by one type of chaotic signal (for example, the received value of x), the logical unit is encoded by another (for example, the value of y);
- nonlinear mixing-the information signal is involved in the formation of the chaotic signal itself.

In the case of the first two algorithms, it is assumed that the parameters of the beginning of key generation by the cryptosystem are chosen randomly to ensure the uniqueness of the key for each block of encrypted data. This implies the need for secure transmission of this data to the receiving side to synchronize the generators.

The solution of the problem of transmitting the parameters of the beginning of key generation (time parameter t, parameters of virtual capacitors x, y and inductance z, or one or more of these parameters) involves the use of asynchronous encryption algorithms, effective and reliable for these purposes due to the small length of the transmitted parameters.

In the case of nonlinear mixing, it is possible to partially refuse to transfer the synchronization parameters of the generators, for example, to transfer only the parameter that was not used to encrypt the data block. Nonlinear mixing and chaotic masking are best used to encrypt data presented in bitwise form in order to compress it, since the omission of bit zero in the decryption process will be easy to detect due to the continuity of the generator function. However, data compression features are not within the scope of this article.

You can use a mixture of the above encryption algorithms.

It is necessary to take into account the probability of turning the parameter superimposed on the information signal to zero or getting zero as a result of nonlinear mixing, because depending on the implementation of the mathematical model of the Chua scheme and the encryption algorithm, there is a probability of turning the encrypted data fragment to zero, which can lead to data loss.

The use of asynchronous encryption algorithms defines this system as a hybrid cryptosystem and allows you to use the best features of both methods of information security, asynchronous encryption and encryption on the chaos generator.

The system can be used to encrypt any kind of information.

Based on the above analysis, a software module used in the encrypted text message transmission system was developed and implemented. The sequence diagram of the use case "Read message" of this system is shown in fig. 4.

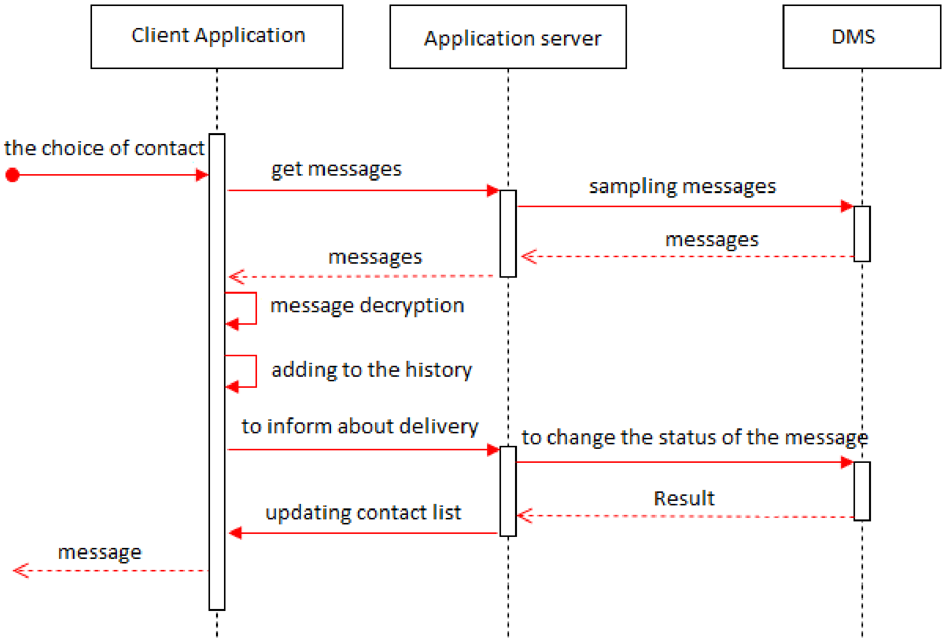

Fig. 4. Sequence Diagram for the "Read message" use case

As it can be seen from the sequence in the diagram, the cryptosystem module was included in the client application. The application server and DBMS are not involved in the process of encrypting and decrypting messages and are only used to provide communication and data transfer between clients.

Due to the use of the chaotic masking algorithm in the module, based on the exclusive "OR" operation (XOR), the same function was used for encryption and decryption, since XOR allows both to mix the key to the data and delete it without changes in the code (unlike, for example, the addition "And" operation, which requires further subtraction to restore the original message).

Synchronization of client application cryptosystems is performed using a session key (in this case, the time parameter t of the chaos generator), transmitted by the asymmetric encryption method.

Conclusion

The review of the literary data, the analysis of publications and researches shows the prospects of creation and application of cryptosystems on chaos generators, in particular on the basis of the Chua scheme. This scheme has typical chaos generators behavior and properties combined with relative ease of implementation. Based on the theory of cryptographic strength of ciphers, systems on chaos generators are the closest to absolutely stable, since the key length can significantly exceed the message length and the uniqueness of its sequence is also high.

On the basis of the analysis, recommendations for the creation of cryptosystems using chaos generators were proposed and substantiated, and a cryptosystem module used in the transmission of encrypted messages was developed.

The objectives of further research is to improve the existing cryptosystem, including changing and improving the mathematical model of the generator used.

References

1. Kocarev, L. & Lian, S. (2011). Chaos-Based Cryptography Theory, Algorithms and Applications. Springer-Verlag, ISBN 978-3-642-20541-5, Berlin, Germany.
2. Chua, L. O.; Wu, C. W.; Huang, A. & Zhong (1993). A universal circuit for studying andgenerating chaos. I. Routes to chaos. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol.40, No.10, (October 1993), pp. 732-744, ISSN 1057-7122
3. Yang, T.; Chai, W. W. & Chua, L. O. (1997). Cryptography based on chaotic systems. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol.44, No.5, (May 1997), pp. 469 - 472, ISSN 1057-7122.
4. Kennedy, M. P. (1994). Chaos in the Colpitts oscillator. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol.41, No.11, (November 1994), pp. 771-774, ISSN 1057-7122.
5. Šalamon, M. & Dogša, T. (1995). Analysis of chaos in the Chua's oscillator. Electrotechnical review: journal of electrical engineering and computer science, Vol.62, No.1, (October1995), pp. 50-58, ISSN 0013-5852.