DOI 10.31489/2019M2/141-148

UDC 004.772

B.K. Shayakhmetova[1], T.L. Ten[2], G.D. Kogay[3], Sh.E. Omarova[2]

[1] *Ye.A. Buketov Karaganda State University, Kazakhstan;*
[2] *Karaganda Economic University of Kazpotrebsoyuz, Kazakhstan;*
[3] *Karaganda State Technical University, Kazakhstan*
(E-mail: tentl@mail.ru)

Models of interaction of cryptography and chaotic dynamics

Cryptography deals with the problem of information protection by its transformation, providing the protection of information (by means of computational techniques), i.e. a set of agreed encryptian tools. Under the cryptosystem in the narrow sense we will understand dynamical systems with a nonlinear function and spatial states, it is represented by a differential equation. Some conditions of the dynamic system, the Lyapunov exponent, as a measure of sensitivity are considered. Identification of the interconnection between objects of study in the theory of chaos and cryptography is revealed; the conclusions about the possibility of using the trajectory of dynamical systems with the chaos for the representation and the transmission of information.

Keywords: cryptography, information protection, encryption, nonlinear function, dynamical system, cryptosystem, parameters, trajectory, transformation, chaotic system, measure of sensitivity.

Introduction

Cryptography deals with the protection of information data through its transformation. Cryptography solves the problems of confidentiality, integrity, authentication, and a number of others that are associated with them. Cryptography actually examines methods for encrypting information, generating digital signatures, and key management certificates.

A cryptographic system, in a broader sense, is an infrastructure that guarantees the protection of information data by means of computer technology, a set of coordinated methods of encryption, transfer and key management, authentication and other elements. A cryptosystem is a hardware-software complex that interacts with a person. It should be noted that scientists working on the protection of information in the conditions of deterministic chaos, the formation of models and descriptions of software applications: E.N. Lorenz [1], M.S. Baptista [2], A. Abel, W. Schwarz [3], K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz [4], K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz [5], L. Kocarev, U. Parlitz [6], Jr.E. Rosa, S. Hayes, C. Grebogi [7], I.P. Marino, Jr.E. Rosa, C. Grebogi [8], I.P. Marino, L. Lopez, M.A.F. Sanjuan [9], L. Kocarev, K.S. Halle, K. Eckert, L. Chua, U. [10], A. Dmitriev, A. Panas, S. Starkov [11], L.A.B. Torres, L.A. Aguirre [12], A.Yu. Loskutov, A.I. Shishmarev [13], A.Yu. Loskutov, V.M. Tereshko, K.A. Vasiliev [14], L. Mariot, A. Leporati, L. Manzoni, G. Mauri, A.E. Porreca, C. Zandron [15], L. Mariot, A. Leporati, A. Dennunzio, E. Formenti [16], A. Leporati [17], L. Mariot, S. Picek, A. Leporati, D. Jakobovic [18].

Purpose of the study. Analyze the relationship for the transmission and presentation of information in terms of cryptography between chaos and objects of complex dynamic systems.

Material and research methods

In the mathematical representation, the cryptosystem $S = (X, Y, K, f)$ is a kind of information conversion $f : X \times K \to Y$, set on the sets of initial states X, keys K and final states Y. The state $x \in X$ encodes some useful information. The sets $X = Y = \subset \{0,1\}*, K \subset \{0,1\}*$ had been studied in computer cryptography, and the transformation f had been studied by means of an algorithm (program) implemented on a Turing machine.

Transformation f is studied as iterations of a cryptographic algorithm (Fig. 1). In this case, the cryptosystem implements a sequence of the set of states $x_0, x_1, ..., x_i, ...$, where $x_i = f(x_{(i-1)}, k) = f^i(x_0, k), x_0 \in X, k \in K$, and the sequence of the set of states is called the system trajectory in Figure 1. The entire trajectory to the same is found by the parameter k and the initial state of the system x_0.

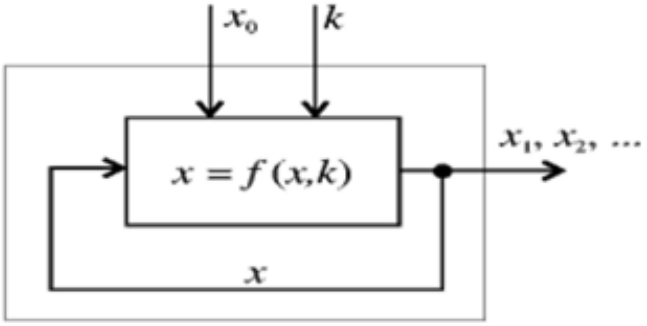


Figure 1. Model of a cryptosystem

The successive transformation of the system states as a result of the use of a certain elementary function of the same type$f$ can be observed in in-line and block ciphers, one-way functions, and pseudorandom number generators. These systems are components of a cryptosystem in a broad sense [19].

The cryptosystem, in a broader sense, is a dynamic system $\langle f, X, k\rangle$ with a non-linear function f, the state space X and the parameter space K.

The dynamic system of continuous time and continuous state $S = \langle X, K, f\rangle$, depends on the parameters and is given in the form of a differential equation:

$$\frac{dx}{dt} = f(x,k), x \in X \subseteq R^d, k \subseteq K \subseteq R^{dk}, \tag{1}$$

where $f : X \times K \to Y$ is a smooth vector function, K is the space of control parameters and X is the state space. The system (1) for a separate initial requirement x_0 satisfies the requirement of the presence and uniqueness of the solution $x \ \ (t, x_0) = x_0$, where $x \ \ (0, x_0) = x_0$. The curve $\varphi_t(t, x_0)$ corresponding to this solution is a trajectory.

The dynamic system of discrete time (continuous state) can be specified as an iterative function:

$$x_{n+1} = f(x_n, k), x_n \in X \subseteq R^d, k \subseteq R^{dk}, \quad n = 0, 1, 2, ..., \tag{2}$$

where x_i is discrete states of the system. The trajectory $\varphi(i, x_0)$ is a sequence of the set $x_0, x_1, ...$ Expression (2), you could notice that it seems with a cryptographic iteration function used in block ciphers, in cryptographic and dynamic systems, pseudo-random generators, studied in iterative transformation of information data that depend on the parameter [20]. Then, the parameter k is reduced in the notation of the system (X, f), and the iteration function $f(x)$. The result of the n-times use of $f(x)$ is written in the form:

$$x_n = f((...(x_0)...)) = f^n(x_0), x_0, x_n \in X.$$

Researchers identify some properties under which chaotic behavior occurs in the system. Namely, the required criterion is made by two classical features — topological transitivity and sensitivity to the initial requirements.

The definition of «chaotic system» has the following interpretation: a dynamic system $\langle X, f\rangle$ is considered chaotic when the following criteria are met:

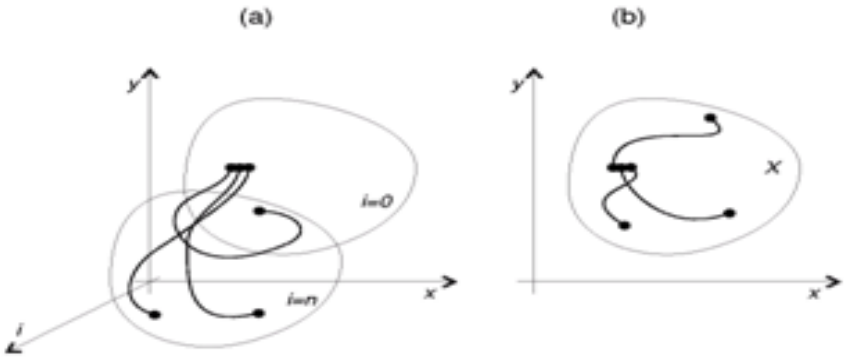
1) The function f is sensitive to the initial criteria, if there is $\delta > 0, n \geq 0$, that for different $x \in X$and its neighborhood H_x there is $y \in H_x$ for which

$$f^n(x) - f^n(y) \vee \sigma;$$

2) The function $f : X \to X$ on some metric set is topologically transitive $X \subset R_d$, if for different open sets $U, V \subset X$ there are $n \geq 0$, such as

$$f^n(U) \bigcap V \neq 0.$$

A dynamic system, in other words, is called chaotic, if all its trajectories are the limit, but instantly diverge at each point of the phase space (Fig. 2).



a) Temporary space; (b) Phase space

Figure 2. Two-dimensional chaotic system

The results of the study and their discussion. The above examples of cryptosystems are similar to chaotic systems: topological transitivity is necessary, firstly, to maintain the state of the cryptosystem within the limits allowed by the information carrier, to «cover» the entire set of ciphertext states as well. The susceptibility to the initial conditions corresponds to the susceptibility of a cryptosystem to a pseudo-random generator or plaintext. From here, as in cryptography, and in the theory of chaos, they come into contact with systems in which even a small change in the initial conditions leads to significant changes along the entire trajectory.

The concept of susceptibility to initial conditions is introduced into the understanding of a chaotic system. This indicator, as a Lyapunov exponent $\lambda(x_0)$, determined for each point $x \in X$, becomes a measure of susceptibility, in other words, determines the speed of the exponential divergence of trajectories, which are located in the vicinity of point x_0

$$f^n(x_0 + \varepsilon) - f^n(x_0) \vee \varepsilon * \varepsilon^{n\lambda(x_0)}$$

in a one-dimensional system where ε is a small deviation from the initial state of the point x_0, and n is a certain number of iterations (or discrete time). For the general case, the value of λ depends on the initial conditions of the point x_0, hence the definition of the averaged value is necessary. For systems that preserve measure, λ is constant for all trajectories. Lyapunov's indicator, in practice, can be calculated as the limit

$$\lambda(x_0) = \lim_{x\to\infty} \lim_{t\to\infty} \frac{1}{n} \vee \frac{f^n(x_0 + \varepsilon) - f^n(x_0)}{\varepsilon} \vee;$$

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{k}^{n} \log \vee f'(x_k) \vee \lim_{n\to\infty} \frac{1}{n} \prod_{k-1}^{n} (x_k) \vee .$$

The derivative $f'(x_k)$, for each k, sets how soon the function f will change relative to the growth of the value of the argument from x_k to x_{k+1}. The limit will be equal to the average value of the logarithm of the derivative after n performed iterations and will show the value of the rate of divergence of the trajectories during the discrete time period. A positive indicator ($\lambda > 0$) is an indicator of the chaotic behavior of the system [21].

For a d-dimensional system, the set $\lambda = \{\lambda_1, ..., \lambda_d\}$ is formed and a more complex behavior is created that is not qualitatively different from the one-dimensional case.

To take into account the accuracy (resolution) of observation, the Kolmogorov-Sinai-h_{KS} entropy, given below, becomes more necessary information.

The value of the Lyapunov indicator, from the point of view of cryptography, becomes a measure of the cryptographic efficiency of the system. More precisely, the larger the value of λ, the smaller the number of iterations needed to obtain a given degree of mixing or spraying information. Existing traditional cryptosystems (pseudo-random generators, encryption schemes) should be studied as dynamic systems that transform information (Table).

Table

Relationship between objects of study in cryptography and chaos theory

Cryptography	Chaos theory
Pseudo-chaotic system	Chaotic system
-finite number of states	-infinite number of states
-finite number of iterations	-infinite number of iterations
-nonlinear transform	-nonlinear transform
Plaintext	Initial state
Key	Initial conditions and parameters
Entanglement	Asymptotic independence of the initial and final states
Ciphertext	Final state
Spraying	Sensitivity to initial conditions and parameters, mixing

From the side of objects and research accents between the theory of chaos and cryptography there are fundamental differences:

1) cryptography analyzes the obtained result of a finite number of iterative transformations ($n < \infty$), as chaos theory (discrete and continuous) studies the asymptotic behavior of the system ($n \to \bullet\infty$);

2) in cryptography it is advised to use all sorts of combinations for independent variables (the system is as unpredictable as possible) and work with spaces with integer dimensions (Fig. 3). Regarding classical chaotic systems, they are displayed in the form of some object or set of phase space, which is endowed with a fractional dimension (in essence, is a fractal);

3) in computer cryptography, the study of a system is carried out at a certain finite number of states, and the multiple state space of a chaotic system is formed with an infinite set of continuous or discrete values. It follows that absolutely all the models of chaos implemented on a computer are very approximate [22].

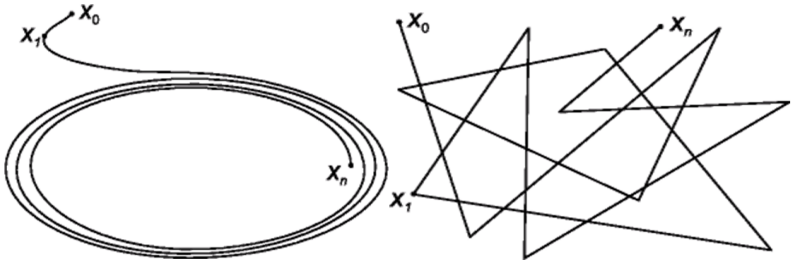


Figure 3. Phase portraits of the chaotic and cryptographic systems

Optimal security (perfect security) of an object will take place only in the situation when it is completely unpredictable for a cryptanalyst (external observer). All of this implies that the likely outcomes (all states) are very equiprobable and are not dependent on past states. In other words, the sequence of states is established by a uniform law of probability distribution and it does not have patterns (correlations). The term «absolute unpredictability» is equivalent to the concept of «true chance». Random sequence is called «white noise». The source of this white noise can be the chaotic system itself, with a rather large number of degrees of freedom (for example, a closed system with a so-called ideal gas).

Certain practical security in the current world is formed by cryptography systems, which, to some extent, will be less than ideal (due to operational and economic feasibility). The definitions of unpredictability and randomness are respectively replaced by polynomial (computational) and pseudo-randomness, unpredictability. A pseudo-random object should not at all differ from a truly random object obtained by means of computational facilities available to an external observer. By analogy, the behavior of a computationally unpredictable object cannot be predicted by the computational means used by the observer. From here, you can prove that a pseudo-random object will be computationally unpredictable.

Therefore, a truly random object will be pseudo-random and algorithmically random. The definitions of algorithmic randomness are also different from each other: pseudo-randomness: a compact generator creates

a pseudo-random string, but an external observer cannot predict the sequence and create this generator. The Universe, nature and matter appear as natural chaos, possessing colossal dimensionality, lack of coverage of the «system of iterative functions» and an infinite number of states. The entropy of these systems, thanks to self-organization, is much less than that of the «completely random» system of a corresponding scale. Multidimensional and chaotic systems cannot be used in encryption, since they are not reproduced. Key generation (without the possibility of repetition), on the other hand, through «natural» chaos (for example, the thermal noise of a computer in a system unit) is widely used today [23].

The deterministic chaos that we use in encryption is endowed with a very small dimension and an infinite number of states. Obviously, such systems are likely to be more predictable than the variant of natural chaos, and they can be modeled by humans in computing systems. To create a calculated estimate of the randomness of such systems, we will make a consistent consideration of the Kolmogorov-Sinai entropy (tightly interconnected with the Lyapunov exponent and algorithmic complexity) and find, moreover, that deterministic chaos leads algorithmically random sequences. In the mixing system, even more so, the numerical sample $x_n, x_{n+k}, x_{n+2k}, x_{n+3k}...$ will be asymptotically ($k \to \infty$) random, that is, with an increase in the value of k, the members of the sample become all less dependent.

Conclusions

Thus, in our analysis, we found a close relationship between the objects of study in chaos theory and cryptography; the conclusion is made with evidence about the apparent probability of applying the trajectory of dynamic systems with chaos for the transmission and presentation of information:

1) the well-known and studied signs of chaotic systems (ergodicity, exponential divergence of trajectories, mixing) can also be fully applied in cryptography for the development of new encryption schemes;

2) the choice of the value of the control parameter in cryptographic applications makes it possible to set the unpredictability of the system, in other words, if the chaotic mapping parameter is used as the key, then the entire space of the probable keys for the assumption of keys is required to correspond to the chaotic one.

References

1 Lorenz E.N. Deterministic Nonperiodic Flow / E.N. Lorenz // J. Athmos. Sci. — 2000. — 20. — P. 130.

2 Baptista M.S. Cryptography with chaos / M.S. Baptista // Phys. Lett. A. — 1998. — 240. — P. 50-54.

3 Abel A. Chaos communication principles, schemes, and system analysis / A. Abel, W. Schwarz // Proc. IEEE. — 2002. — 90. — No. 5. — P. 691–710.

4 Cuomo K.M. Synchronization of Lorenz-based chaotic circuits with application to communications / K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz // IEEE Trans. Circ. Syst. II. — 1993. — 40. — No. 10. — P. 626–633.

5 Cuomo K.M. Circuit implementation of synchronized chaos with applications to communications / K.M. Cuomo, A.V. Oppenheim // Phys. Rev. Lett. — 1993. — 71, No. 1. — P. 65–68.

6 Kocarev L. General approach for chaotic synchronization with applications to telecommunication / L. Kocarev, U. Parlitz // Phys. Rev. Lett. — 1995. — 74, No. 25. — P 5028–5031.

7 Rosa Jr. E. Noise ltering in communication with chaos / Jr.E. Rosa, S. Hayes, C. Grebogi // Phys. Rev. Lett. — 1997. — 78, No. 7. — P. 1247-1250.

8 Marino I.P. Exploiting the natural redundancy of chaotic signals in communication systems / I.P. Marino, Jr.E. Rosa, C. Grebogi // Phys. Rev. Lett. — 2000. — 85, No. 12. — P. 2629–2632.

9 Marino I.P. Channel coding in communications using chaos / I.P. Marino, L. Lopez, M.A.F. Sanjuan // Physics Letters A. — 2002. — 295, No. 4. — P. 185–191.

10 Kocarev L. Experimental demonstration of secure communications via chaotic synchronization / L. Kocarev, K.S. Halle, K. Eckert, L. Chua, U. Parlitz // Int. J. Bifurcation and Chaos. — 1992. — 2, 3. — P. 709.

11 Dmitriev A. Experiments on speech and music signals transmission using chaos / A. Dmitriev, A. Panas, S. Starkov // Int. Journal of Bifurcation and Chaos. — 1995. — 5, 4. — P. 1249–1254.

12 Torres L.A.B. Extended chaos control method applied to Chua circuit / L.A.B. Torres, L.A. Aguirre // Electronics Letters. — 1999. — 35. — No. 10. — P. 768–770.

13 Loskutov A.Yu. Control of dynamical systems behavior by parametric perturbations an analytic approach / A.Yu. Loskutov, A.I. Shishmarev // Chaos. — 2004. — 4. — No. 2. — P. 351–355.

14 Loskutov A.Yu. Stabilization of chaotic dynamics of one-dimensional maps by cyclic parametric transformation / A.Yu. Loskutov, V.M. Tereshko, K.A. Vasiliev // Int. J. Bi. and Chaos. — 2006. — 6, No. 4. — P. 725–735.

15 Leporati A.C. Characterizing the complexity of tissue P systems with fission rules / A.C. Leporati, L. Manzoni, G. Mauri, A.E. Porreca, C. Zandron // Journal of Computer and System Sciences. — 2017. — 90. — P. 115-128.

16 Mariot L.A. Computing the periods of preimages in surjective cellular automata / L.A. Mariot, A. Leporati, A. Dennunzio, E. Formenti, // Natural Computing. — 2017. — 16, No. 3. — P. 367–381.

17 Mariot, L.A cryptographic and coding-theoretic perspective on the global rules of cellular automata / L.A. Mariot, A. Leporati // Natural Computing. – 2018. – 17. – №3. – P. 487-498.

18 Mariot L.A. Cellular automata based S-boxes / L.A. Mariot // Cryptography and Communications. — 2019. — 11, No. 1. — P. 41–62.

19 Колесов В.В. Шифрование цифровой информации при использовании генераторов с хаотической динамикой / В.В. Колесов, Н.Н. Залогин, Г.М. Воронцов // РЭ. — 2008. — 53, № 4, — С. 459–467.

20 Птицын Н. Приложение детерминированного хаоса в криптографии / Н. Птицын. — М.: Изд-во Москов. техн. ун-та им. Н.У. Баумана, 2009. – С. 70.

21 Марков А.С. Конвергенция средств защиты информации / А.С. Марков, А.А. Фадин // Защита информации: Инсайд. — 2013. — № 4. — С.53–55.

22 Бейсенби М.А., Тайлак Б.Е., Томилова Н.И. Формализация взаимосвязи детерминированного хаоса и криптографии // Фундаментальные и прикладные исследования, разработка и применение высоких технологий в промышленности: материалы XIII Междунар. науч.-практ. конф. — СПб.: СПб НИУ ИТМО, 2012. — С. 168–171.

23 Когай Г.Д. Криптографические системы по управлению детерминированным хаосом / Г.Д. Когай, Т.Л. Тен // Гамбург, 2014. — С. 132-134.

Б.К. Шаяхметова, Т.Л. Тен, Г.Д. Когай, Ш.Е. Омарова

Криптография және хаос динамиканың өзарабайланыс модельдері

Криптография ақпаратты қорғауды қамтамасыз ететін (есептеуіш техника құралдары арқылы) оны түрлендіру жолымен ақпаратты қорғау мәселесімен айналысады, яғни келісілген шифрлау құралдарының жиынтығы. Тар мағынада криптожүйе — сызықты емес функциясы және кеңістік жағдайлары бар динамикалық жүйе, әдетте ол дифференциалдық, теңдеумен ұсынылған. Динамикалық жүйенің кейбір шарттары, сезімталдық өлшемі ретінде Ляпунов көрсеткіші қарастырылды. Хаос және криптография теориясындағы зерттеу нысандары арасындағы өзара байланыс анықталды; ақпаратты ұсыну және беру үшін хаос пен динамикалық жүйелердің траекториясын пайдалану мүмкіндіктері туралы қорытынды жасалды.

Кілт сөздер: криптография, ақпаратты қорғау, шифрлеу, бейсызық функция, динамикалық жүйе, криптожүйе, параметрлер, траектория, түрлендіру, хаотикалық жүйе, сезімталдық мөлшері.

Б.К. Шаяхметова, Т.Л. Тен, Г.Д. Когай, Ш.Е. Омарова

Модели взаимосвязи криптографии и хаотической динамики

Криптография занимается проблемой защиты информации путем ее преобразования (средствами вычислительной техники), т.е. является совокупностью согласованных средств шифрования. Под криптосистемой в узком смысле будем понимать динамическую систему с нелинейной функцией и пространством состояний, обычно она представлена дифференциальным уравнением. Рассмотрены некоторые условия динамической системы, показатель Ляпунова как мера чувствительности. Выявлена взаимосвязь между объектами изучения в теории хаоса и криптографии; сделаны выводы относительно возможности использования траектории динамических систем с хаосом для предоставления и передачи информации.

Ключевые слова: криптография, защита информации, шифрование, нелинейная функция, динамическая система, криптосистема, параметры, траектория, преобразование, хаотическая система, мера чувствительности.

References

1 Lorenz, E.N. (2000). Deterministic Nonperiodic Flow. *J. Athmos. Sci, 20,* 130.

2 Baptista, M.S. (1998). Cryptography with chaos. *Phys. Lett. A., 240,* 50-54.

3 Abel, A., & Schwarz, W. (2002). Chaos communication principles, schemes, and system analysis. *Proc. Ieee, 90, 5,* 691-710.

4 Cuomo, K.M., Oppenheim, A.V., & Strogatz, S.H. (1993). Synchronization of Lorenz-based chaotic circuits with application to communications. *Ieee Trans. Circ. Syst. II, 40, 10,* 626-633.

5 Cuomo, K.M., & Oppenheim, A.V. (1993). Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett., 71, 1,* 65-68.

6 Kocarev, L., & Parlitz, U. (1995). General approach for chaotic synchronization with applications to telecommunication. *Phys. Rev. Lett., 74, 25,* 5028-5031.

7 Rosa, Jr.E., Hayes, S., & Grebogi, C. (1997). Noise ltering in communication with chaos. *Phys. Rev. Lett., 78, 7,* 1247-1250.

8 Marino, I.P., Rosa, Jr.E., & Grebogi, C. (2000). Exploiting the natural redundancy of chaotic signals in communication systems. *Phys. Rev. Lett., 85, 12,* 2629-2632.

9 Marino, I.P., Lopez, L., & Sanjuan, M.A.F. (2002). Channel coding in communications using chaos. *Physics Letters A, 295, 4,* 185-191.

10 Kocarev, L., Halle, K.S., Eckert, K., Chua, L., & Parlitz, U. (1992). Experimental demonstration of secure communications via chaotic synchronization. *Int. J. Bifurcation and Chaos, 2, 3,* 709-713.

11 Dmitriev, A., Panas, A., & Starkov, S. (1995). Experiments on speech and music signals transmission using chaos. *Int. Journal of Bifurcation and Chaos, 5, 4,* 1249-1254.

12 Torres, L.A.B., & Aguirre, L.A. (1999). Extended chaos control method applied to Chua circuit. *Electronics Letters, 35,10,* 768-770.

13 Loskutov, A.Yu., & Shishmarev, A.I. (2004). Control of dynamical systems behavior by parametric perturbations an analytic approach. *Chaos, 4, 2,* 351-355.

14 Loskutov, A.Yu., Tereshko, V.M., & Vasiliev, K.A. (2006). Stabilization of chaotic dynamics of one-dimensional maps by cyclic parametric transformation. *Int. Journal of Bifurcation and Chaos, 6, 4,* 725-735.

15 Leporati, A., Manzoni, L., Mauri, G., Porreca, & A.E., Zandron, C. (2017). Characterizing the complexity of tissue P systems with fission rules. *Journal of Computer and System Sciences, 90,* 115-128.

16 Mariot, L., Leporati, A., Dennunzio, A., & Formenti, E. (2017). Computing the periods of preimages in surjective cellular automata. *Natural Computing, 16, 3,* 367-381.

17 Mariot, L., & Leporati, A. (2018). A cryptographic and coding-theoretic perspective on the global rules of cellular automata. *Natural Computing, 17, 3,* 487-498.

18 Mariot, L., Picek, S., Leporati, A., & Jakobovic, D. (2019). Cellular automata based S-boxes. *Cryptography and Communications, 11, 1,* 41-62.

19 Kolesov, V.V., Zalogin, N.N., & Vorontsov, G.M. (2008). Shifrovanie tsifrovoi informatsii pri ispolzovanii heneratorov s khaoticheskoi dinamikoi [Encryption of digital information using generators with chaotic dynamics]. *RE, 53, 4,* 459-467 [in Russian].

20 Ptitsyn, N. (2009). *Prilozhenie determinirovannoho khaosa v kriptohrafii [Application of deterministic chaos in cryptography].* Maoscow: Izd-vo Mosk. tekh. univ. im. N.U. Baumana [in Russian].

21 Markov, A.S., & Fadin, A.A. (2013). Konverhentsiia sredstv zashchity informatsii [Convergence of information protection means]. *Zashchita informatsii. Insaid, 4,* 53-55 [in Russian].

22 Beisenbi, M.A., Taylak, B.E., & Tomilova, N.I. (2012). Formalizatsiia vzaimosviazi determinirovannoho khaosa i kriptohrafii [Formalization of the relationship of deterministic chaos and cryptography]. *Materials of the XIII International Scientific and Practical Conference «Fundamental and applied research, development and application of high technologies in industry».* Saint Petersburg: St. Petersburg NRU ITMO[in Russian].

23 Kogay, G.D., & Ten, T.L. (2014). Kriptohraficheskie sistemy po upravleniiu determinirovannym khaosom [Cryptographic systems for managing deterministic chaos]. *Hamburg*, 218, 132-134 [in Russian].