Chaos, Solitons and Fractals 133 (2020) 109615

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

journal homepage: www.elsevier.com/locate/chaos

# Adaptive chaotic maps and their application to pseudo-random numbers generation

Aleksandra V. Tutueva[a], Erivelton G. Nepomuceno[b], Artur I. Karimov[c], Valery S. Andreev[a], Denis N. Butusov[c,*]

[a] Department of Computer-Aided Design, Saint Petersburg Electrotechnical University "LETI", 5, Professora Popova st., Saint Petersburg 197376, Russia
[b] Control and Modelling Group (GCOM), Department of Electrical Engineering, Federal University of São João del-Rei, São João del-Rei, MG 36307-352, Brazil
[c] Youth Research Institute, Saint-Petersburg Electrotechnical University "LETI", 5, Professora Popova st., Saint Petersburg 197376, Russia

ARTICLE INFO

*Article history:*
Received 5 July 2019
Revised 17 October 2019
Accepted 29 November 2019

*Keywords:*
Chaotic discrete map
Zaslavsky web map
Adaptive symmetry
Chaos-based cryptography
Pseudo-random generator

ABSTRACT

Chaos-based stream ciphers form a prospective class of data encryption techniques. Usually, in chaos-based encryption schemes, the pseudo-random generators based on chaotic maps are used as a source of randomness. Despite the variety of proposed algorithms, nearly all of them possess many shortcomings. While sequences generated from single-parameter chaotic maps can be easily compromised using the phase space reconstruction method, the employment of multi-parametric maps requires a thorough analysis of the parameter space to establish the areas of chaotic behavior. This complicates the determination of the possible keys for the encryption scheme. Another problem is the degradation of chaotic dynamics in the implementation of the digital chaos generator with finite precision. To avoid the appearance of quasi-chaotic regimes, additional perturbations are usually introduced into the chaotic maps, making the generation scheme more complex and influencing the oscillations regime. In this study, we propose a novel technique utilizing the chaotic maps with adaptive symmetry to create chaos-based encryption schemes with larger parameter space. We compare pseudo-random generators based on the traditional Zaslavsky map and the new adaptive Zaslavsky web map through multi-parametric bifurcation analysis and investigate the parameter spaces of the maps. We explicitly show that pseudo-random sequences generated by the adaptive Zaslavsky map are random, have a weak correlation and possess a larger parameter space. We also present the technique of increasing the period of the chaotic sequence based on the variability of the symmetry coefficient. The speed analysis shows that the proposed encryption algorithm possesses a high encryption speed, being compatible with the best solutions in a field. The obtained results can improve the chaos-based cryptography and inspire further studies of chaotic maps as well as the synthesis of novel discrete models with desirable statistical properties.



## 1. Introduction

It is known, that there is a close relationship between the properties of deterministic chaos and the requirements imposed on cryptographic systems [1]. According to the concept proposed by Shannon, any cryptographic system should implement the confusion and diffusion processes [2]. In chaotic systems, those processes match with ergodicity, a mixing property and high sensitivity to the small variations of initial conditions or control parameters. Therefore, the chaos phenomenon can be a prospective pseudo-random source in data encryption schemes.

Like their classical counterparts, chaos-based cryptographic systems can be classified into two groups: stream ciphers and block ciphers. Since stream encryption schemes usually have a higher encryption speed they can be effectively used in real-time applications. The common way to construct a stream cipher is the generation of a pseudo-random sequence to mask a plaintext [3]. Many encryption schemes that use chaos-based pseudo-random number generators (PRNG) have been recently proposed [3–23]. Despite the variety of described algorithms, many of them possess several common shortcomings. First, some of the described schemes employ one-dimensional chaotic maps [3,8,9] and therefore are vulnerable to attacks based on the phase space reconstruction method [11,13]. In addition, the set of keys is essentially limited for one-dimensional chaotic maps with a single parameter, since usually the initial conditions and nonlinearity parameter are the only available encryption keys [5]. For instance, schemes based

* Corresponding author.
*E-mail addresses:* avtutueva@etu.ru (A.V. Tutueva), nepomuceno@ieee.org (E.G. Nepomuceno), aikarimov@etu.ru (A.I. Karimov), vsandreev@etu.ru (V.S. Andreev), dnbutusov@etu.ru (D.N. Butusov).

https://doi.org/10.1016/j.chaos.2020.109615
0960-0779/

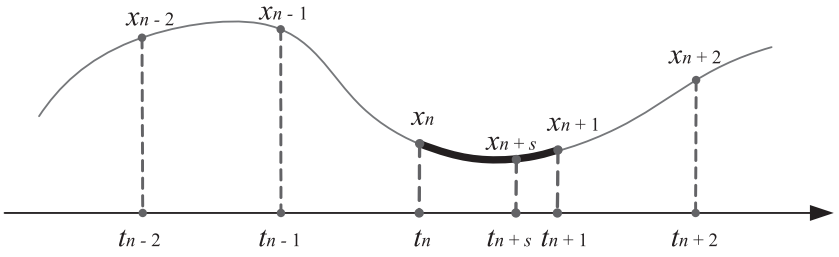


**Fig. 1.** Geometric interpretation of the adaptive symmetry technique.

on the logistic map allow obtaining pseudo-random sequences for a parameter with values in the interval [3.57; 4]. However, when applying maps with a higher number of parameters, it becomes necessary to determine the parameter boundaries where the resulting sequence is still chaotic. When several parameters are used simultaneously as a part of the key, the mutual interdependence complicates the choice of regions in the key space and should be avoided [24].

Another issue of chaos-based PRNG arises in the implementation of chaos generators with finite precision. Many researchers have studied the influence of a data type to the period length of chaotic sequences [5,10,25–28]. Data type limitations impoverish chaotic dynamics and cause the appearance of short-period orbits. Hence, the security of the final cryptographic system can be significantly reduced [24]. To solve the aforementioned problem several techniques were proposed [29–32]. The obvious way is to implement generators with higher precision [29], but this can significantly slow down the computations. Another solution is the implementation of chaotic cascades [32], which complicates the generation algorithm and increases the overhead costs. One of the prospective ideas is to use the perturbation-based algorithms [30,31], using the nonlinearity parameter as a subject for the perturbation. Thus, it is necessary to check the type of oscillations of nonlinear system (periodic or chaotic) while the nonlinear parameter changes.

In this paper we propose a new approach to the pseudo-random generation based on the novel concept of chaotic maps with adaptive symmetry. Since the adaptive coefficient practically does not affect the nature of the system this opens up great opportunities for improving known chaos-based PRNG. The adaptive coefficient is not a bifurcation parameter, so it can be assumed that additional multi-parametric analysis will not be required. Moreover, symmetry coefficient can be changed to contribute complementary perturbations, thereby increasing the period length of chaotic sequences.

The rest of the paper is organized as follows. In Section 2 we propose the method for constructing chaotic maps with variable symmetry and introduce the adaptive Zaslavsky web map as an example. Section 3 shows the application of chaotic maps with adaptive symmetry to the stream ciphers and presents the results of multi-parametric bifurcation and correlation analysis of sequences generated by the PRNG based on the Zaslavsky web map. Finally, some conclusions and discussion are given in Section 4.

## 2. Adaptive chaotic maps

In previous paper [33] we considered the symmetric versions of the well-known Chirikov and Henon maps. These maps were generated through the application of geometric integration techniques to the continuous dynamical systems. The conventional way to integrate the Hamiltonian system is to apply the single-step single-stage Euler-Cromer integration operator, which results in symplectic, but not symmetric integration scheme. Applying a composition of two adjoint Euler-Cromer methods, we can use the additional integration point at the time $t_n + 0.5h$, where $h$ is the discretization step. In the proposed adaptive maps one can change this additional integration point by varying the symmetry coefficient $S$ (Fig. 1) without loss of chaotic properties. The case $S = 1$ corresponds to single-stage Euler-Cromer scheme and $S = 0.5$ corresponds to the symmetric integration (Verlet scheme). In other cases, as we will show below, the value of symmetry coefficient can be changed almost arbitrarily. Let us consider the proposed approach for the Zaslavsky map.

The Zaslavsky map appears in the literature in at least two different versions. The first one is a dissipative generalization of the standard map [34]. It is determined by the following equations

$$\begin{aligned} y_{n+1} &= \{y_n + \nu(1 + \mu z_n) + \epsilon\nu\mu\cos(2\pi y_n)\}; \\ z_{n+1} &= e^{-r}(z_n + \epsilon\cos(2\pi y_n)); \end{aligned} \tag{1}$$

and

$$\nu = \frac{1 - e^{-r}}{r}$$

where $y$, $z$ are dimensionless coordinates, $\epsilon$ is the dimensionless parameter of the perturbation, $r$ is the dissipation parameter, the brackets {} denote the fractional of the argument.

Another version is the stochastic web map, also known as Zaslavsky map. The Zaslavsky web map is a model exhibiting minimal chaos, i.e., a special case of chaotic motion that implies the existence of small chaotic regions in a phase space of the system under infinitesimally small perturbations [35]. Let us consider a linear pendulum affected by an infinite wave set whose dynamics can be described as follows

$$\begin{pmatrix} q_{n+1} \\ p_{n+1} \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} q_n \\ p_n + K\sin q_n \end{pmatrix}. \tag{2}$$

where $q$ and $p$ are dimensionless coordinates between two successive kicks, $K$ is the intensity of the kicks, $\alpha$ is the frequency.

Resonant cases when $\alpha = 2\pi/m$, $m \in Z$ are of a special interest because they let the system exhibit minimal chaos. The phase portrait of the system in this state represents a stochastic web, a pattern of thin channels separating isolated regions of regular dynamics [36]. The stochastic webs of Zaslavsky map (2) are shown in Fig. 2. These stochastic webs possess a fractal structure and have resemblance with crystal grids [22]. Cases of $m = 4$ and $m = 6$ are called trivial resonances since they generate stochastic webs with a very simple regular structure, while cases of $m = 5, 7, 8, 9, \ldots$ are called non-trivial resonances and their stochastic webs resemble oriental ornaments based on $m$-beam stars.

To obtain the adaptive Zaslavsky map, let us consider a symmetric version of the original map. One of the possible symmetric forms can be described as follows:

$$\begin{pmatrix} q_{n+1} \\ p_{n+1} \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \cdot \left( \begin{pmatrix} q_n \\ p_n + 0.5\,K\sin q_n \end{pmatrix} + \begin{pmatrix} 0 \\ 0.5\,K\sin q_{n+1} \end{pmatrix} \right)$$

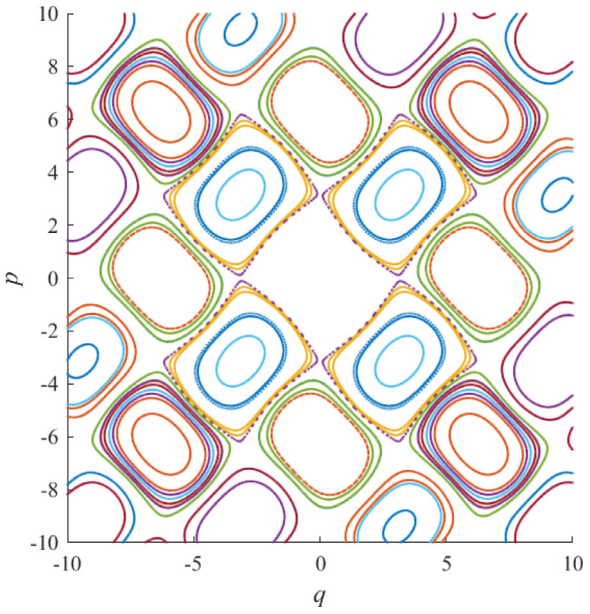


**Fig. 2.** The phase space of the Zaslavsky web map for $K = 0.8$ and $m = 4$, the case of the trivial resonance.

Applying the adaptive integration technique we obtain

$$\begin{pmatrix} q_{n+1} \\ p_{n+1} \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} q_n \\ p_n + SK\sin q_n + (1-S)K\sin q_{n+1} \end{pmatrix} \tag{3}$$

where $S$ is the symmetry coefficient.

Phase space of system (3) with various values of $S$ is shown in Fig. 3. For a case of a trivial resonance with $S = 0.5$ (Fig. 3c), one can see the shape of stochastic cells in the given scale. The shape of the cells becomes symmetric with respect to axes $p = 0$ and $q = 0$.

In the next section, the application of obtained map to the pseudo-random generation in chaos-based stream ciphers will be considered.

## 3. Adaptive Zaslavsky web map in pseudo-random number generation

As it was previously stated, when implementing a chaos-based stream cipher it is necessary to determine the intervals of the parameter values, which give key space of the resulting encryption scheme. The introduction of adaptive symmetry into chaotic maps simplifies this task. Let us compare the PRNG based on the Zaslavsky (1) map [37] and the generator based on the Zaslavsky web map with adaptive symmetry (3). We transformed the real number to a sequence of 0 and 1 with the following formula

$$b = \mod(abs(integer(x \cdot 10^9)), 2) \tag{4}$$

where $abs(x)$ is the absolute value of $x$ and $integer(x)$ is a function of reducing $x$ to an integer value. The concatenation of $b$ values gives the output sequence of the PRNG. The initial values for the pseudo-random number generation using the Zaslavsky chaotic map are usually chosen from the interval [0; 1] [37].

### 3.1. Bifurcation analysis

The choice of the parameters of chaotic generator is usually based on parametric dynamical analysis. The most common tool is a dynamical map of the system, where parameter values are plotted on the axis and the color corresponds to the largest Lyapunov exponent (LLE) for a couple of system parameters [24,38]. The dynamical map of the system (1) is given in Fig. 4. The black color corresponds to the parameter values that should be avoided when implementing a PRNG to keep the encryption scheme secure. One can note that precise definition of boundaries for these areas is a non-trivial task because any change in parameters sufficiently influences the system behavior. Studies of Avrutin, Schanz et al. [39,40] show that simultaneous changes in the parameter values can lead to the appearance of special types of multi-parametric bifurcations. To determine the conditions where they occur, new methods still need to be developed.

Let us consider the dynamical map for the Zaslavsky web map with adaptive symmetry where $m = 4$ (Fig. 5). The parameter $K$ and the symmetry coefficient $S$ are plotted along the horizontal and vertical axes, respectively. One can see that for values of $K$ that exceed 2.5, the behavior of the considered system is chaotic for any $S$. One can observe the same changes in the oscillation regimes in original Zaslavsky web map.

The detailed study [33] of symmetric and non-symmetric maps has shown that changing the symmetry is an isomorphic transform and provides phase space stretching and compression without affecting the chaotic behavior. Therefore one can assume that when the symmetry coefficient is simultaneously changed along with the system bifurcation parameter, undesirable $n$-parametric bifurcations will not occur. This fact theoretically provides a larger key space to the PRN generators based on adaptive symmetric maps.

### 3.2. Key space analysis

The key space is a vital feature of chaos-based cryptographic systems. In paper [37] B. Stoyanov and K. Kordov do not discuss the size of the key space. The proposed generator was based on a map (1) with two nonlinearity parameters and two initial conditions. These four values were represented using a floating-point data type [41] with precision of $p = 53$ bits, which yields $2^{212}$. The generation algorithm proposed in this paper is based on chaotic map (3), and possess the same number of key parameters. It is believed that a secure cryptosystem must have a key space larger than $2^{100}$ to be robust against brute-force attacks [42–44]. Hence, both approaches provide a key space that is larger than the required minimum. In order to approximately determine the key space boundaries which correspond to the positive LLE values, one can use a simple analysis of dynamical map in Fig. 5 roughly estimating the percentage of white spots. For pseudo-random generators based on adaptive maps, this task can be easier than for traditional chaos-based generators. Moreover, for encryption schemes with single-parameter maps such as the Chirikov map [45], the inclusion of an adaptive coefficient will at least double the size of the key space.

### 3.3. Correlation analysis

Many previous studies that considered PRNG based on the Zaslavsky map, represented only the results of randomness test for the generated sequences. In our study we also perform a comparative correlation analysis to experimentally show that sequences obtained by the adaptive Zaslavsky web map do not change the type of behavior while the symmetry coefficient value is changed.

We used Eq. (4) for converting the phase variable values into the bit sequence. All calculations were carried out with double precision IEEE floating-point numbers. First, we investigated the correlation of sequences generated from close initial points. Following Stoyanov and Kordov [37], we generated the sequence of length $10^5$. To obtain new sequences we shifted this point $10^3$ times to

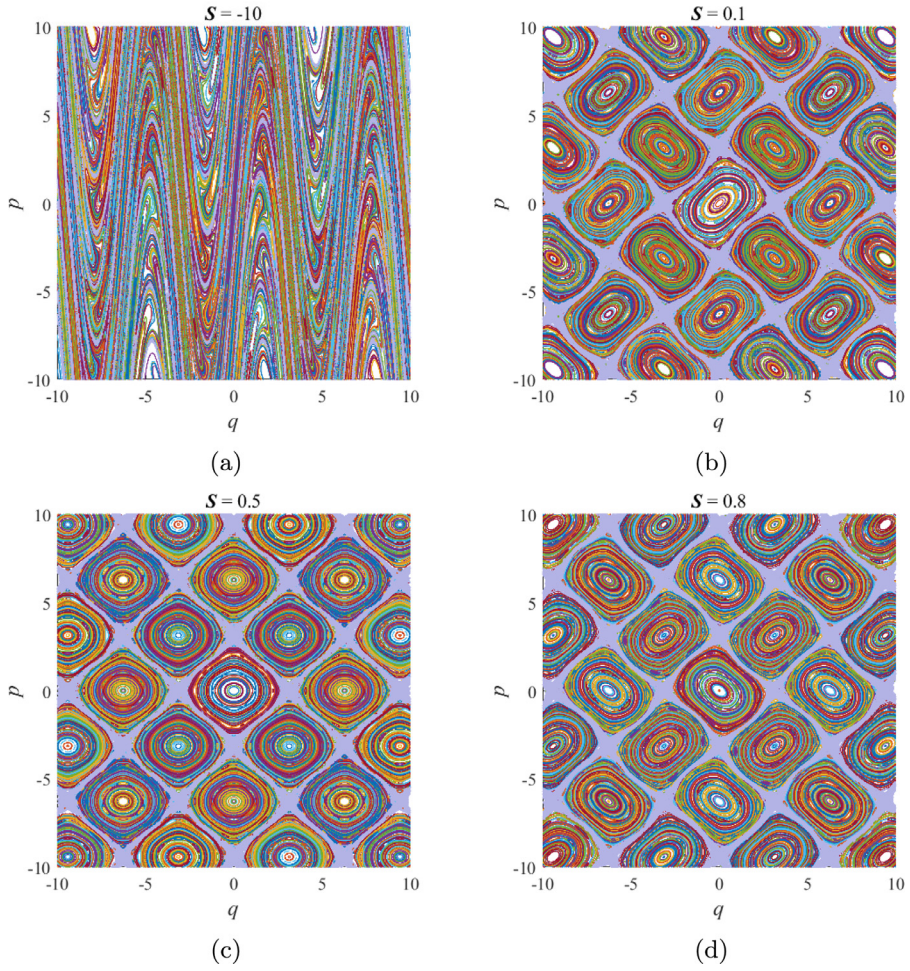


**Fig. 3.** Phase space of adaptive Zaslavsky web maps for $K = 1.2$ and $m = 4$ with: (a) $S = -10$; (b) $S = 0.1$; (c) $S = 0.5$; (d) $S = 0.8$. Light-violet color corresponds to the net-shaped chaotic sea. (To see full color figures, the reader is referred to the web version of this article.)

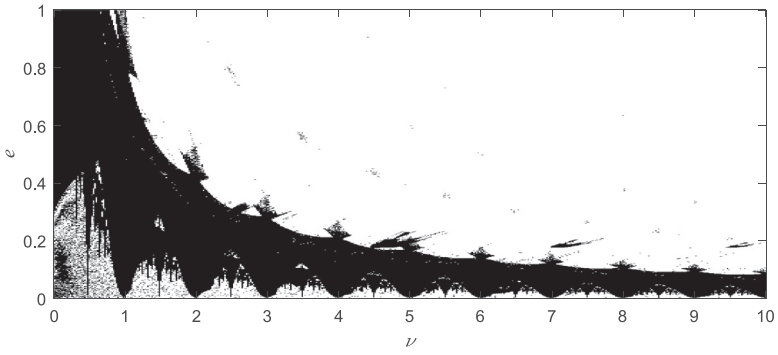


**Fig. 4.** The dynamical map for Zaslavsky map (1) while $e \in [0; 1]$ and $\nu \in [0; 10]$. Negative values of LLE correspond to black color, positive values to white.

the machine epsilon. For the final set we calculated the values of the Pearson correlation coefficients and obtained their distribution (Figs. 6–8). One can see, the obtained values do not exceed 0.02 for all generators including the original Zaslavsky generator (Fig. 6), which corresponds to a weak correlation according to the Chedock scale. Thus, we can claim that the correlation of the generated sequences does not depend on the symmetry coefficient.

On the next step we investigated the correlation between the sequences obtained by maps starting at one initial point with the small differences in the symmetry coefficient. Setting the starting point as 0.5, we added the machine epsilon to $S$ $10^3$ times and generated sequences of length $10^5$. Then we calculated the Pearson correlation coefficient for all obtained sequences. Fig. 9 represents the final distribution. The results are similar to those obtained in the previous experiment. Sequences generated with close values of the symmetry coefficient have a weak correlation relationship, which indicates that the symmetry coefficient can be considered as a key.

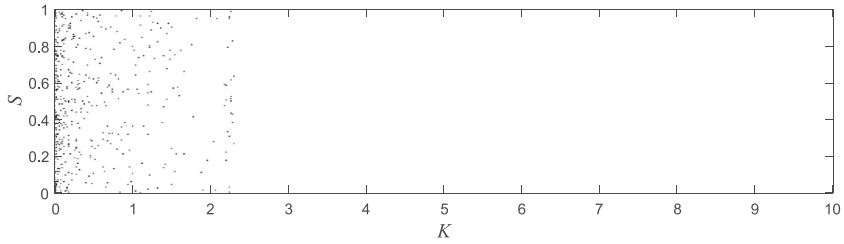


**Fig. 5.** The dynamical map for the adaptive Zaslavsky web map (3) while $S \in [0; 1]$ and $K \in [0; 10]$. Negative LLE values correspond to black color, positive LLE values are marked white.

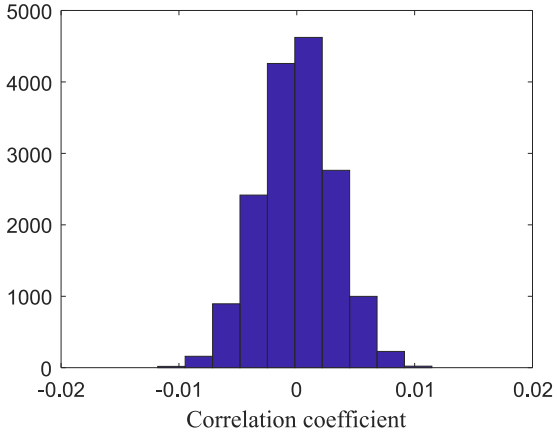


**Fig. 6.** The distribution of the Pearson correlation coefficient calculated for the sequences generated by PRNG based on the original Zaslavsky map with $r = 3, \nu = 400/3, e = 0.3$.

Both experiments have shown that the change of the symmetry coefficient does not affect the correlation properties of the sequences obtained by the PRNG based on the adaptive map. That corresponds well with the theoretical predictions.

### 3.4. Statistical testing

Another common approach to investigate pseudo-random sequences is the statistical testing. In 2001, the National Institute of Standards and Technology (NIST) published a general methodology for PRNG testing intended for this purpose [46]. We used this technique to study the proposed generator based on the Zaslavsky web map with adaptive symmetry. We performed the experiments with different values of the symmetry coefficient using the NIST test suite implemented in LabVIEW 2018. A set of 100 sequences with a length of $10^6$ bits each (the minimum length recommended for NIST testing) was studied. The level of significance $\alpha$ in our experiments was 0.01. The obtained results are shown in Table 1. One can see that the investigated generator produces sequences with random characteristics for all of the considered cases.

A detailed analysis of the dependence between the symmetry coefficient and sequences is of interest for further research.

### 3.5. Encryption speed analysis

The recent studies have shown that the efficiency of traditional cryptographic schemes, including widely used Advanced Encryption Standard (AES), is relatively low in the case of multimedia data encryption [47]. One of the possible advantages of chaotic cryptography is higher encryption speed [48].

To estimate the performance of chaos-based schemes we compared the encryption speed of the stream cipher based on the proposed PRNG and the AES algorithm. We chose the AES implementation from the Crypto Toolkit developed by Alab Technologies for NI LabVIEW. For the AES encryption, the key length was 128 bit and the block cipher mode of operation was Cipher Block Chaining (CBC). We varied the number of bytes of data for encryption and estimated the time costs. For each data set, we performed 100 executions that were averaged. The obtained results are shown in Fig. 10. One can see that the chaos-based encryption is faster than the traditional approach. The averaged encryption speed for the proposed algorithm is 315 B/ms. Gayathri and Subashini [48] presented the comparison of the encryption speed for different chaos-based cryptosystems (See Table 7 in [48]). The authors investigated eight algorithms based on different chaotic maps. Only two of them show better encryption speed than the proposed cipher based on the adaptive map (2023 B/ms for the Kanso cipher [49], 407.1 B/ms for the Zhou cipher [50]). However, the Zhou cipher is based on the one-dimensional logistic map that

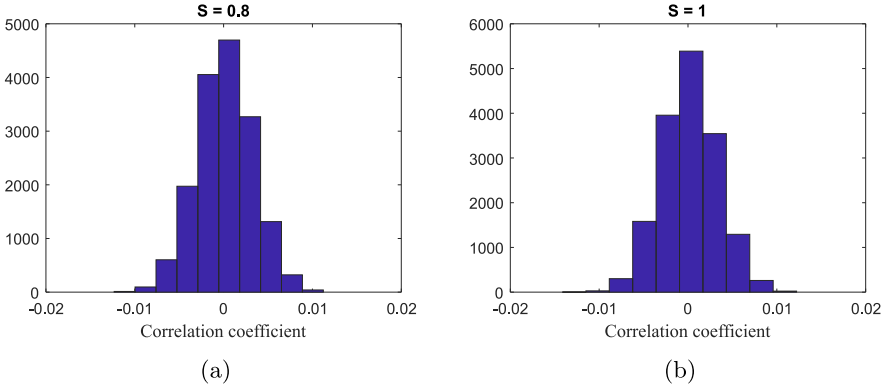


**Fig. 7.** The distribution of the Pearson correlation coefficient calculated for the sequences generated by the PRNG based on the Zaslavsky web map with adaptive symmetry with $K = 3$ and (a) $S = 1$; (b) $S = 0.8$.

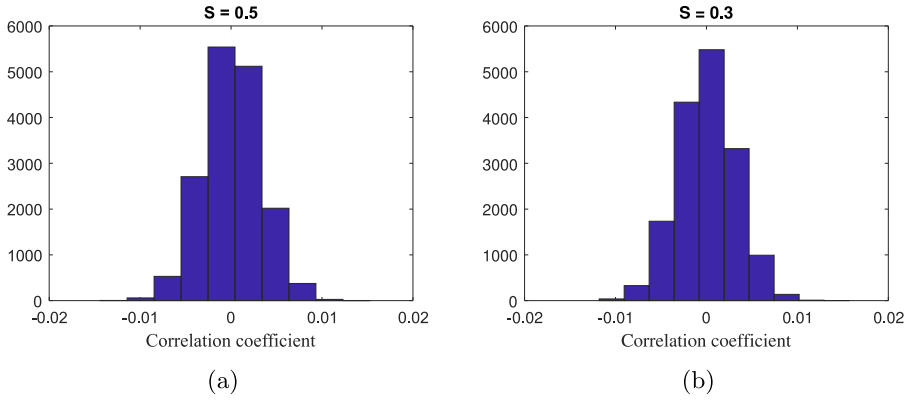


**Fig. 8.** The distribution of the Pearson correlation coefficient calculated for the sequences generated by the PRNG based on the Zaslavsky web map with adaptive symmetry with $K = 3$ and (a) $S = 0.5$; (b) $S = 0.3$.

**Table 1**
Results of NIST testing for PRNG based on the adaptive Zaslavsky map with $K = 3$.

| Statistical tests | $S = 0.3$ | | $S = 0.5$ | | $S = 0.8$ | | $S = 1$ | |
|---|---|---|---|---|---|---|---|---|
| | *Pvalue* | Pass rate | *Pvalue* | Pass rate | *Pvalue* | Pass rate | *Pvalue* | Pass rate |
| FT | 0.025 | 0.99 | 0.367 | 1 | 0.475 | 1 | 0.319 | 0.99 |
| BFT | 0.046 | 0.98 | 0.304 | 1 | 0.596 | 1 | 0.720 | 0.97 |
| CST | 0.475 | 0.99 | 0.351 | 1 | 0.367 | 1 | 0.534 | 0.99 |
| RT | 0.055 | 0.99 | 0.575 | 1 | 0.616 | 1 | 0.437 | 0.99 |
| LROT | 0.115 | 1 | 0.049 | 0.98 | 0.978 | 1 | 0.911 | 1 |
| MRT | 0.004 | 1 | 0.575 | 0.99 | 0.494 | 1 | 0.575 | 1 |
| SPT | 0.851 | 0.98 | 0.086 | 0.98 | 0.575 | 0.99 | 0.225 | 0.99 |
| NTMT | 0.109 | 0.99 | 0.401 | 0.99 | 0.740 | 0.98 | 0.616 | 0.98 |
| OTMT | 0.086 | 0.99 | 0.262 | 0.99 | 0.616 | 0.98 | 0.956 | 1 |
| MUST | 0.202 | 0.98 | 0.437 | 0.99 | 0.760 | 0.99 | 0.350 | 0.98 |
| AET | 0.049 | 0.98 | 0.779 | 1 | 0.021 | 1 | 0.637 | 0.99 |
| RET | 0.616 | 0.98 | 0.740 | 0.99 | 0.658 | 1 | 0.575 | 1 |
| REVT | 0.554 | 1 | 0.081 | 0.99 | 0.145 | 0.99 | 0.679 | 0.99 |
| ST | 0.122 | 0.99 | 0.514 | 1 | 0.401 | 1 | 0.834 | 1 |
| LCT | 0.049 | 0.99 | 0.817 | 0.99 | 0.554 | 0.97 | 0.091 | 1 |

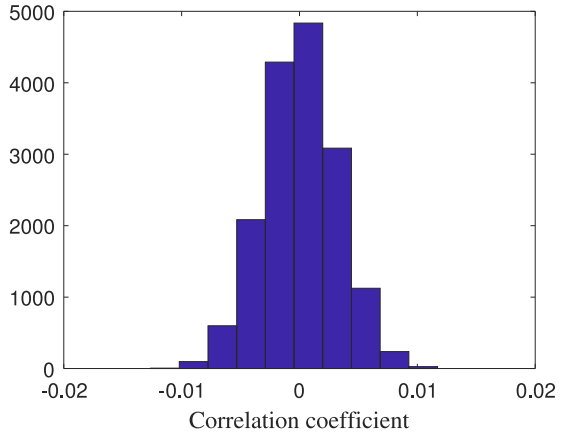


**Fig. 9.** The distribution of the Pearson correlation coefficient calculated for the sequences generated by the PRNG based on the Zaslavsky map with adaptive symmetry where $S$ value was varied linearly.

not able to resist the attack by the method of the phase space reconstruction. The Kanso algorithm uses the three-dimensional cat map as the pseudo-randomness source. The chaotic behavior of this map significantly depends on the parameter matrix which includes six values. This problem has already been discussed in detail in Section 3.1. Thus, the proposed algorithm is devoid of such shortcomings and shows a high encryption speed (Fig. 11).

### 3.6. The adaptive coefficient as a perturbation

It is possible to increase the complexity of the chaotic behavior by introducing a function that changes the symmetry coefficient during the simulation. As it was shown before, the linear changes of the symmetry coefficient result in an infinitesimally small correlation of the generated sequences. Thus, replacing the coefficient $S$ by a function we can make the phase space of the system more complex. This also can notably deform the areas of chaotic sea and stability islands without changing other parameters of the map [33]. Actually, this brings us to a new family of discrete maps based on initial symmetric prototype.

Let us consider the Zaslavsky web map with a resonance $\alpha = \pi/4$ which corresponds to 8-beam symmetry in the phase space. For the perturbation parameter $K = 0.8$, the chaotic sea is large enough and has star-like shape, allowing the Arnold diffusion to exist for a notable set of initial conditions. When the symmetry coefficient is governed by the law $S = \sin(2\pi/n)$, where $n = 4$ (Fig. 10), the phase space is similar to the case of trivial resonance $\alpha = \pi/2$, but with the shifted axes. The case $n = 9$ (Fig. 10c) shows several embedded chaotic seas, which do not intersect with each other, and the overall chaotic sea area becomes sufficiently larger. The case $n = 3$ (Fig. 10d) corresponds to an even more expanded chaotic sea. If $n$ is irrational, no periodic solutions can be found and thus no stability islands exist. In this case, the chaotic sea occupies the entire phase space.

Note, that the perturbation function can be chosen in an almost arbitrary way. The possibility of obtaining pseudo-random

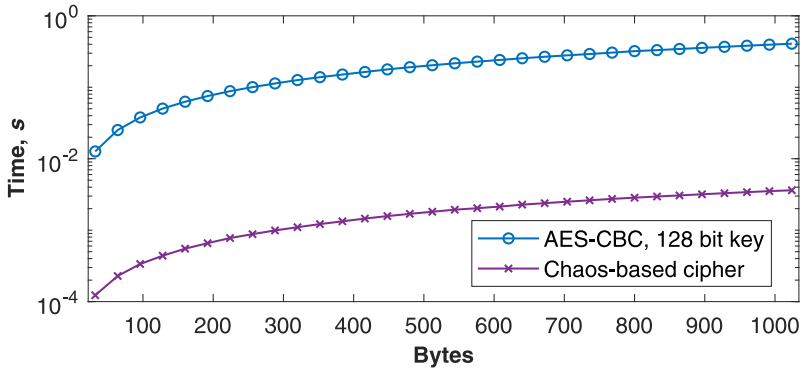


**Fig. 10.** The time costs for data encryption using AES algortihm and chaos-based stream cipher.

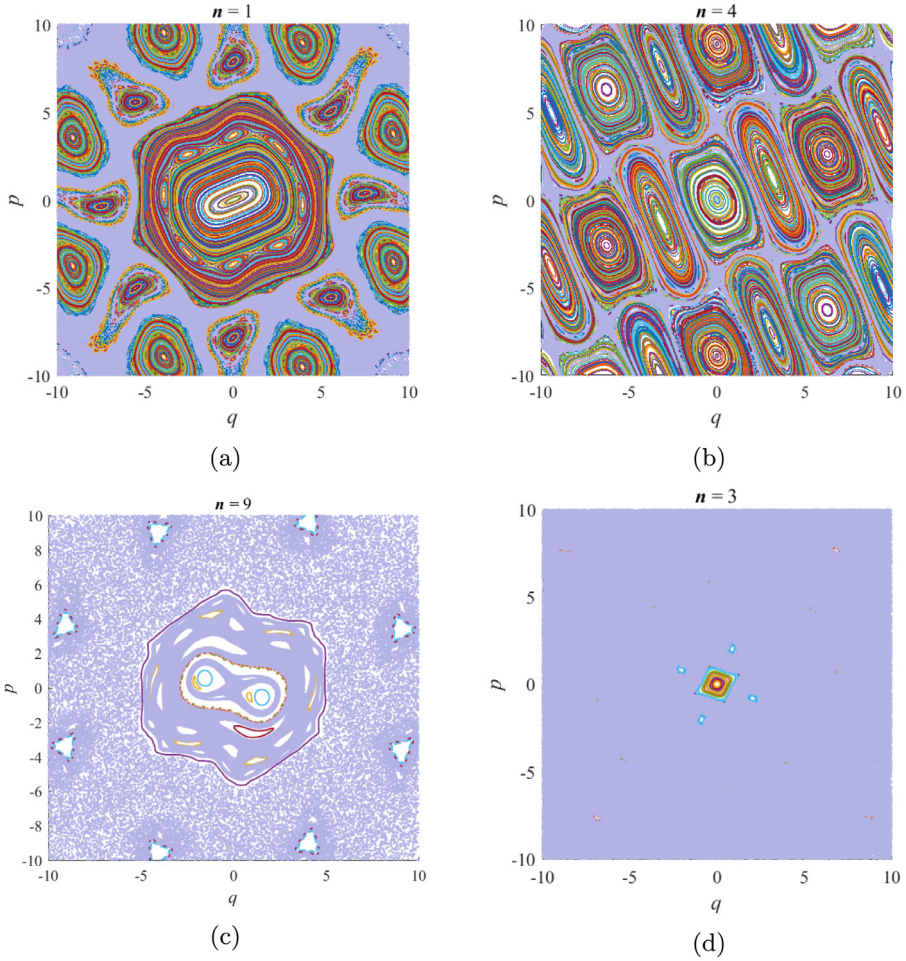


**Fig. 11.** Poincare sections of the adaptive Zaslavsky map with $S = \sin(2\pi/n)$. Light violet color corresponds to chaotic sea. (To see full color figures, the reader is referred to the web version of this article.)

sequences with different values of the adaptive coefficient was confirmed by NIST tests in the previous section.

## 4. Conclusion and discussion

The experimental study of the proposed adaptive Zaslavsky map shows that the sequences generated by the corresponding PRNG have the property of randomness and demonstrate a weak correlation relationship regardless of the values of the symmetry coefficient. This means that the symmetry coefficient can be efficiently used as a key parameter in chaos-based cryptographic schemes, making increase in the key space possible. We also used the idea of the perturbing parameter proposed earlier in [30,31] to develop the technique that make it possible to avoid the short-period quasi-chaotic sequences by varying the symmetry coefficient. We suggested exploiting the symmetry coefficient as a perturbation parameter to obtain novel discrete maps based on the symmetric prototype. The proposed approach allows to increase the period of oscillations because the sequences, generated with close symmetry coefficient values, are loosely coupled. In addition, the computational complexity of the generation scheme does not increase.

Thus, we can conclude that chaotic maps with adaptive symmetry are suitable for the stream ciphers. The PRNG based on the

adaptive map described in this paper is easier to implement than the previously known modified chaos-based generators. The increase in encryption speed can be estimated only after a thorough security analysis of the final cryptographic scheme. In our further studies we will explore various attacks on the cryptographic system based on the adaptive maps, including an attack by phase space reconstruction. Another direction for future research is a search for other applications of maps with adaptive symmetry, where this property can be effectively used. One of them can be the application of the adaptive symmetry concept to the models based on coupled map lattices and networks, including artificial neural networks. We will also consider the development of other adaptive maps, the synchronization of adaptive symmetric chaotic systems and obtaining sequences with certain statistical properties by controllable symmetry.

## Declaration of Competing Interest

None.

## Acknowledgments

Denis N. Butusov was supported by the grant of the Russian Science Foundation (RSCF), project 19-71-00087.

## References

[1] Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia 1989;13(1):29–42.
[2] Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J 1949;28(4):656–715.
[3] Kanso A, Smaoui N. Logistic chaotic maps for binary numbers generations. Chaos Solitons Fractals 2009;40(5):2557–68.
[4] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 1998;8(6):1259–84.
[5] Kotulski Z, Szczepański J, Górski K, Paszkiewicz A, Zugaj A. Application of discrete chaotic dynamical systems in cryptography DCC method. Int J Bifurcation Chaos 1999;9(6):1121–35.
[6] Wang X-Y, Wang X-J. Design of chaotic pseudo-random bit generator and its applications in stream-cipher cryptography. Int J Mod Phys C 2008;19(05):813–20.
[7] Zheng F, Tian X, Song J, LI X. Pseudo-random sequence generator based on the generalized Henon map. J China Univ Posts Telecommun 2008;15(3):64–8.
[8] Som S, Dutta S, Singha R, Kotal A, Palit S. Confusion and diffusion of color images with multiple chaotic maps and chaos-based pseudorandom binary number generator. Nonlinear Dyn 2015;80(1–2):615–27.
[9] Sun F, Liu S. Cryptographic pseudo-random sequence from the spatial chaotic map. Chaos Solitons Fractals 2009;41(5):2216–19.
[10] Persohn K, Povinelli RJ. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation. Chaos Solitons Fractals 2012;45(3):238–45.
[11] Hu H, Liu L, Ding N. Pseudorandom sequence generator based on the Chen chaotic system. Comput Phys Commun 2013;184(3):765–8.
[12] Akhshani A, Akhavan A, Mobaraki A, Lim S-C, Hassan Z. Pseudo random number generator based on quantum chaotic map. Commun Nonlinear Sci Numer Simul 2014;19(1):101–11.
[13] Liu L, Miao S, Cheng M, Gao X. A pseudorandom bit generator based on new multi-delayed Chebyshev map. Inf Process Lett 2016;116(11):674–81.
[14] Lambić D, Nikolić M. Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn 2017;90(1):223–32.
[15] Öztürk I, Kılıç R. A novel method for producing pseudo random numbers from differential equation-based chaotic systems. Nonlinear Dyn 2015;80(3):1147–57.
[16] Wang Y, Liu Z, Ma J, He H. A pseudorandom number generator based on piecewise logistic map. Nonlinear Dyn 2016;83(4):2373–91.
[17] Murillo-Escobar M, Cruz-Hernández C, Cardoza-Avendaño L, Méndez-Ramírez R. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. Nonlinear Dyn 2017;87(1):407–25.
[18] Wang X, Qin X. A new pseudo-random number generator based on CML and chaotic iteration. Nonlinear Dyn 2012;70(2):1589–92.
[19] Wang X, Bao X. A novel block cryptosystem based on the coupled chaotic map lattice. Nonlinear Dyn 2013;72(4):707–15.
[20] Meranza-Castillón M, Murillo-Escobar M, López-Gutiérrez R, Cruz-Hernández C. Pseudorandom number generator based on enhanced Hénon map and its implementation. AEU Int J Electron Commun 2019;107:239–51.
[21] Elmanfaloty RA, Abou-Bakr E. Random property enhancement of a 1D chaotic PRNG with finite precision implementation. Chaos Solitons Fractals 2019;118:134–44.
[22] Farsana F, Gopakumar K. A novel approach for speech encryption: Zaslavsky map as pseudo random number generator. Procedia Comput Sci 2016;93:816–23.
[23] Szczepański J, Kotulski Z. Pseudorandom number generators based on chaotic dynamical systems. Open Syst Inf Dyn 2001;8(2):137–46.
[24] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcation Chaos 2006;16(8):2129–51.
[25] Nepomuceno EG, Junior HMR, Martins SA, Perc M, Slavinec M. Interval computing periodic orbits of maps using a piecewise approach. Appl Math Comput 2018;336:67–75.
[26] Nepomuceno EG, Mendes EM. On the analysis of pseudo-orbits of continuous chaotic nonlinear systems simulated using discretization schemes in a digital computer. Chaos Solitons Fractals 2017;95:21–32.
[27] Kovalevsky DV, Kuzmina SI, Bobylev LP. Impact of nonlinearity of climate damage functions on long-term macroeconomic projections under conditions of global warming. Discontin Nonlinearity Complex 2015;4(1):25–33.
[28] Karimov TI, Butusov DN, Pesterev DO, Predtechenskii DV, Tedoradze RS. Quasi-chaotic mode detection and prevention in digital chaos generators. In: 2018 IEEE conference of russian young researchers in electrical and electronic engineering (ElConRus). IEEE; 2018. p. 303–7.
[29] Flores-Vergara A, García-Guerrero E, Inzunza-González E, López-Bonilla O, Rodríguez-Orozco E, Cárdenas-Valdez J, et al. Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic. Nonlinear Dyn 2019;96(1):1–20.
[30] Dastgheib MA, Farhang M. A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period. Nonlinear Dyn 2017;89(4):2957–66.
[31] Tong X, Cui M. Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. Signal Process 2009;89(4):480–91.
[32] Kwok H, Tang WK. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solitons Fractals 2007;32(4):1518–29.
[33] Butusov DN, Karimov AI, Pyko NS, Pyko SA, Bogachev MI. Discrete chaotic maps obtained by symmetric integration. Phys A 2018;509:955–70.
[34] Zaslavsky G. The simplest case of a strange attractor. Phys Lett A 1978;69(3):145–7.
[35] Chernikov A, Sagdeev R, Usikov D, Zakharov MY, Zaslavsky G. Minimal chaos and stochastic webs. Nature 1987;326(6113):559.
[36] Zaslavsky GM. Chaos, fractional kinetics, and anomalous transport. Phys Rep 2002;371(6):461–580.
[37] Stoyanov B, Kordov K. Novel Zaslavsky map based pseudorandom bit generation scheme. Appl Math Sci 2014;8(178):8883–7.
[38] Peixoto ML, Nepomuceno EG, Martins SA, Lacerda MJ. Computation of the largest positive Lyapunov exponent using rounding mode and recursive least square algorithm. Chaos Solitons Fractals 2018;112:36–43.
[39] Avrutin V, Schanz M. On multi-parametric bifurcations in a scalar piecewise–linear map. Nonlinearity 2006;19(3):531.
[40] Avrutin V, Schanz M, Banerjee S. Multi-parametric bifurcations in a piecewise—linear discontinuous map. Nonlinearity 2006;19(8):1875.
[41] Kahan W. IEEE standard 754 for binary floating-point arithmetic. Lecture Notes Status IEEE 1996;754(94720-1776):11.
[42] Norouzi B, Mirzakuchaki S. A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dyn 2014;78(2):995–1015.
[43] Hu T, Liu Y, Gong L-H, Ouyang C-J. An image encryption scheme combining chaos with cycle operation for dna sequences. Nonlinear Dyn 2017;87(1):51–66.
[44] Li C, Lin D, Feng B, Lü J, Hao F. Cryptanalysis of a chaotic image encryption algorithm based on information entropy. IEEE Access 2018;6:75834–42.
[45] Stoyanov B, Kordov K. A novel pseudorandom bit generator based on Chirikov standard map filtered with Shrinking rule. Math Probl Eng 2014;2014.
[46] Bassham III LE, Rukhin AL, Soto J, Nechvatal JR, Smid ME, Barker EB, et al. Sp 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications 2010.
[47] Su Z, Zhang G, Jiang J. Multimedia security: a survey of chaos-based encryption technology. In: Multimedia-a multidisciplinary approach to complex issues. InTech; 2012. p. 99–124.
[48] Gayathri J, Subashini S. A survey on security and efficiency issues in chaotic image encryption. Int J Inf Comput Secur 2016;8(4):347–81.
[49] Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. Commun Nonlinear Sci Numer Simul 2012;17(7):2943–59.
[50] Zhou Y, Bao L, Chen CP. A new 1D chaotic system for image encryption. Signal Process 2014;97:172–82.