Adaptive Chirikov Map for Pseudo-random Number Generation in Chaos-based Stream Encryption

Aleksandra Tutueva, Dmitriy Pesterev, Artur Karimov, Denis Butusov, Valerii Ostrovskii
Saint-Petersburg Electrotechnical University "LETI"
Saint-Petersburg, Russia
{avtutueva, dopesterev, aikarimov, dnbutusov, vyostorvskii}@etu.ru

***Abstract*—Information security plays an important role in modern technologies. Stream encryption is one of the common tools used for secure communications. The stream encryption algorithms require sequence with pseudo-random properties. The chaotic maps as a source of pseudo-random numbers with desired statistical properties is widely studied in the last decades. One of the known problems of the implementation of the chaos-based pseudo-random number generators implemented with low-precision arithmetic is a short period length. A possible solution of the short-cycle problem is a perturbation of the orbit or the nonlinearity parameter of the chaotic map for breaking out the cycle. In the present article, we propose a new approach for increasing the cycle length by changing the symmetry coefficient of the adaptive Chirikov map. We switch two values of the symmetry coefficient according to the output of the linear feedback shift register. We calculate the estimations of the period length for the perturbed and original Chirikov maps and confirm the efficiency of the proposed approach. Properties verification for the output sequences of generators based on the adaptive Cirikov map is carried out using correlation analysis methods and the NIST statistical test suite. The obtained results can be used in cryptography applications as well as in secure communication systems design.**

I. Introduction

The chaotic encryption is one of prospective fields of modern cryptography. Ergodicity, a mixing property and high sensitivity to the small variations of initial conditions or control parameters of such systems match with confusion and diffusion processes implemented in most cryptographic systems [1–3]. Chaotic maps as a source of pseudo-randomness in stream encryption ensure high encryption speed. Therefore, chaotic encryption is prospective for the secure processing of multimedia data [4].

One of the common problems of chaos-based ciphers implemented with finite precision is a short period of the chaotic sequence. Considering the logistic map, Persohn in [5] explicitly showed that for 4-bit binary fractions representation, the trajectory starts repeating after two iterations with a period of three for any initial value. One of the prospective techniques for increasing the period is to use the perturbation-based algorithms. In general, such algorithms use an idea of breaking out the short cycle by perturbing the orbit or the nonlinearity parameter of the chaotic system. Hu et al. described various types of perturbation algorithms and estimated their influence on statistical properties of generated chaotic sequences [6]. In [7] it was shown that the switching between two values of the parameter of the logistic map can significantly increase the period. In [8] authors proposed the algorithm based on self-perturbation of the chaotic map. This technique showed good results for low-precision arithmetic in the case of the logistic map simulation.

It can be noted that the nonlinearity parameter is often chosen as a subject for the perturbation. Thus, it is necessary to check the type of oscillations of the nonlinear system (periodic or chaotic) while the parameter changes. To solve this problem, we propose to use adaptive maps with the controllable parameter called the symmetry coefficient. The symmetry coefficient changes a rotation in the phase space and does not affect the nonlinear properties of the system. Moreover, the symmetry coefficient can be a part of the key for chaos-based stream ciphers. Thus, the cryptographic strength of the encryption scheme is potentially increased.

The rest of paper is organized as follows. In Section II, we describe the adaptive Chirikov map and present the symmetry coefficient concept. In Section III, we propose and examine the technique for perturbing the symmetry coefficient to avoid the periodicity. In Section IV, we investigate a pseudo-random generator based on the adaptive Chirikov map and present the results of correlation and statistical analysis of generated pseudo-random sequences. Finally, some conclusions are given in Section V.

II. Adaptive Chirikov map

The standard Chirikov map is the well-known map with chaotic properties [9]. The map equations state the relationship between momentum p and coordinate x:

$$\begin{aligned} p_{n+1} &= p_n + K \sin x_n, \\ x_{n+1} &= x_n + p_{n+1} \end{aligned} \tag{1}$$

where K is the parameter. State space variables are considered modulo 2π.

Butusov [10] and Karimov [11] described the technique to obtain the symmetric version of chaotic maps using semi-implicit integration. Such maps yield reflectional symmetry in the phase space. One of the possible symmetric forms of the Chirikov map can be described as follows

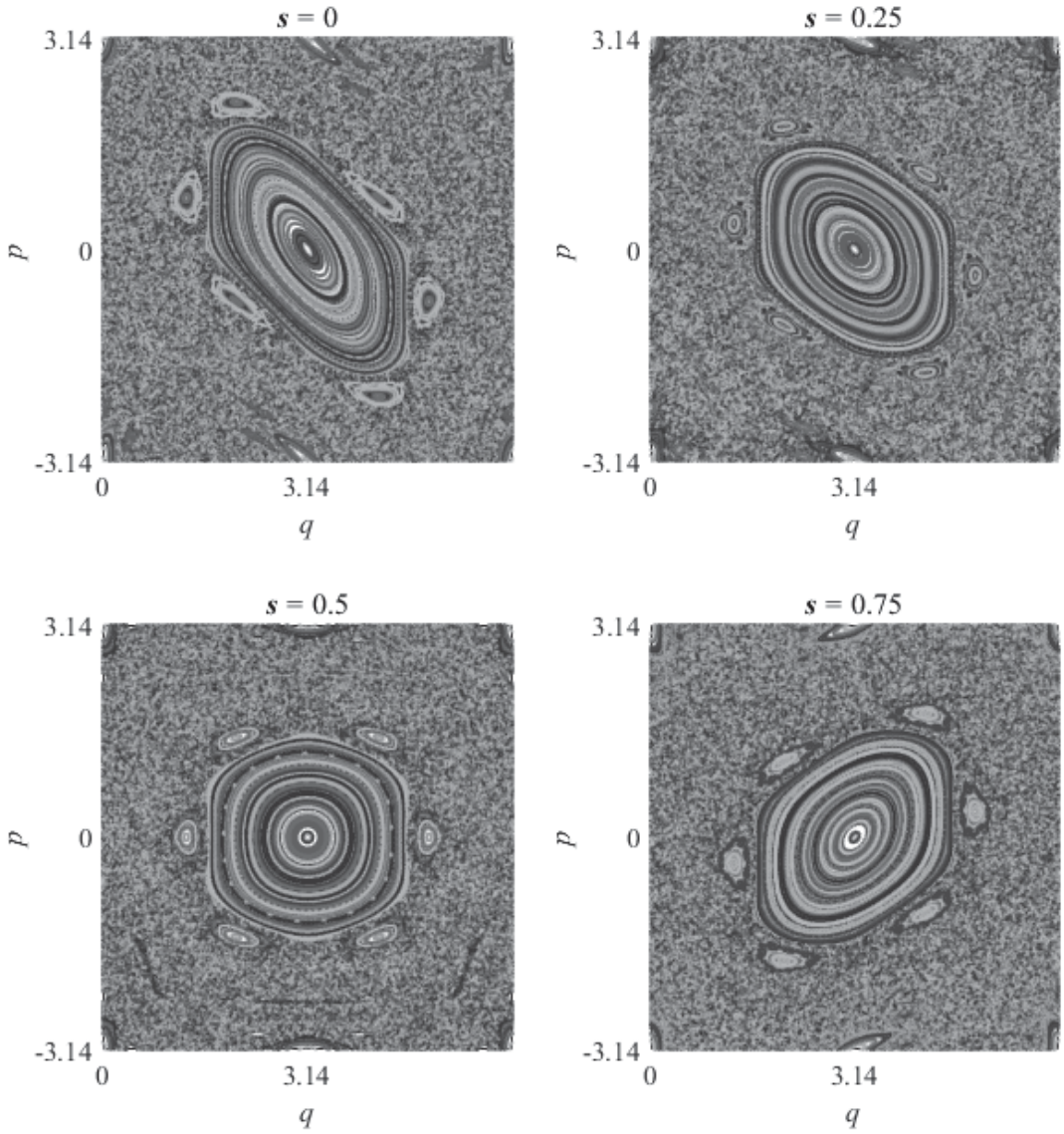

Fig. 1. The adaptive Chirikov map phase portraits for various S

$$\begin{aligned} p_{n+0.5} &= p_n + 0.5K \sin x_n, \\ x_{n+1} &= x_n + p_{n+0.5}, \\ p_{n+1} &= p_{n+0.5} - 0.5K \sin x_{n+1}. \end{aligned} \tag{2}$$

Replacing 0.5 in (2) with the symmetry coefficient S and $(S-1)$ we obtain

$$\begin{aligned} p_{n+s} &= p_n + SK \sin x_n, \\ x_{n+1} &= x_n + p_{n+s}, \\ p_{n+1} &= p_{n+s} - (1-S)K \sin x_{n+1}. \end{aligned} \tag{3}$$

One can change the shape of the phase space of the adaptive Chirikov map varying the symmetry coefficient S (Fig. 1). The perturbation of the symmetry coefficient does not affect the nature of the process but allows to break the short cycles of the chaotic sequence.

III. The Perturbation in theAdaptive Chirikov Map

A. The proposed perturbation technique

The simplest perturbation scheme of the nonlinearity parameter was described by Spenger in [7]. The proposed technique is based on switching between two values every N iterations. The properties of chaos ensure that the changes of parameters values lead to different behavior. The Spenger technique shows good results in calculations with the floating-point data type. However, in fixed-point calculations with a small bit depth, the chaotic sequence can become periodic before the N^{th} iteration. Therefore, we propose to modify this approach and use it to perturb the symmetry coefficient of adaptive maps.

Let us consider two given values of the symmetry coefficient S_1 and S_2. The perturbation of the chaotic map is performed by switching the values of the symmetry coefficient

between S_1 and S_2. To determine the time moments of the changes, the linear feedback shift register (LFSR) is used. S_1 is matched to zero output bit of LFSR, and S_2 to one bit. The proposed scheme with LFSR controlled by primitive polynomial $y^8 + y^6 + y^5 + y^4 + 1$ is presented in Fig. 2.

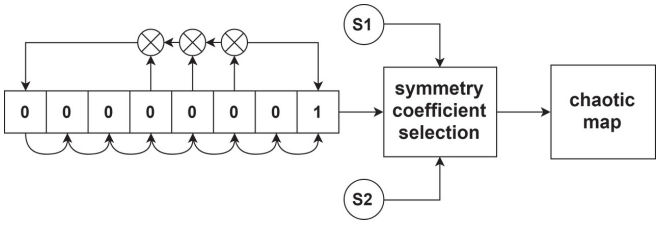

Fig. 2. The adaptive map perturbation process

Let us apply the proposed approach to the adaptive map (3).

B. Bifurcation analysis

The bifurcation diagram is a common tool for the chaotic system investigation. Fig. 3 represents the results of bifurcation analysis of the original Chirikov map and the perturbed adaptive Chirikov map in 16-bit fixed-point implementation (8 bit for the word length). The values of the symmetry coefficients S_1 and S_2 were equal to 1 and 0.5, respectively. In this case, we switched maps (1) and (2). One can see, the proposed technique allow to obtain sequences with chaotic behavior even in the case of small values of K. Moreover, in the original map most of the obtained values are located in the interval $[\pi; 2\pi]$ (Fig. 2, *a*). One can see, that the perturbation of the symmetry coefficient leads to a distribution that is closer to the uniform one (Fig. 2, *b*).

C. Cycle length estimation

To estimate the cycle length we used 16-bit fixed-point data type, as in the previous experiment. We compared the obtained cycle lengths for the original Chirikov map and the perturbed adaptive map while initial values were varied in interval [0.03125; 0.96875] for both variables. For each pair of initial conditions, 500 iterations were calculated with different K. The obtained results are shown in Fig. 4. The white color corresponds to the maximum period, i.e. in this case each sequence value was repeated only once. One can see that the proposed technique is suitable for break out the cycles in chaotic sequences.

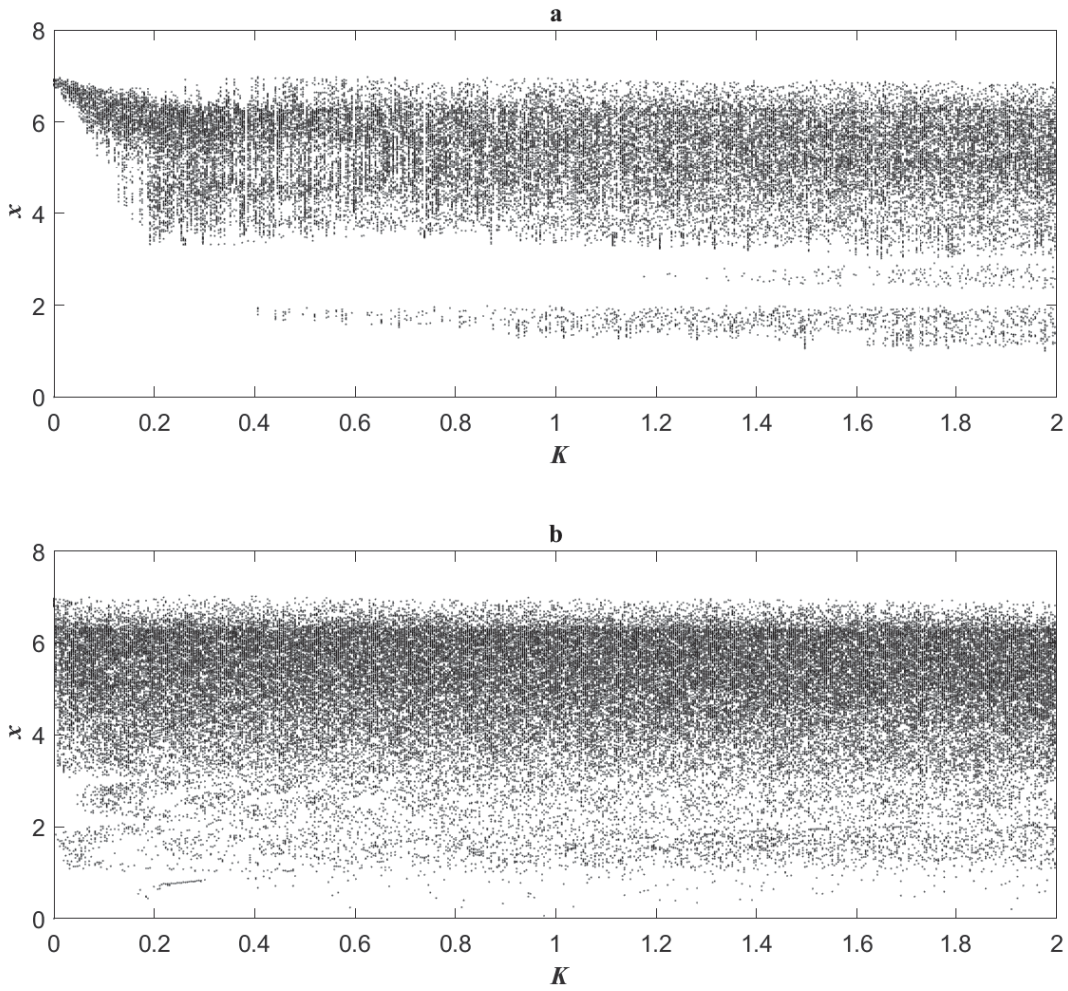

Fig. 3. The bifurcation diagrams for fixed-point implementation of original Chirikov map (a) and the perturbed adaptive Chirikov map (b)

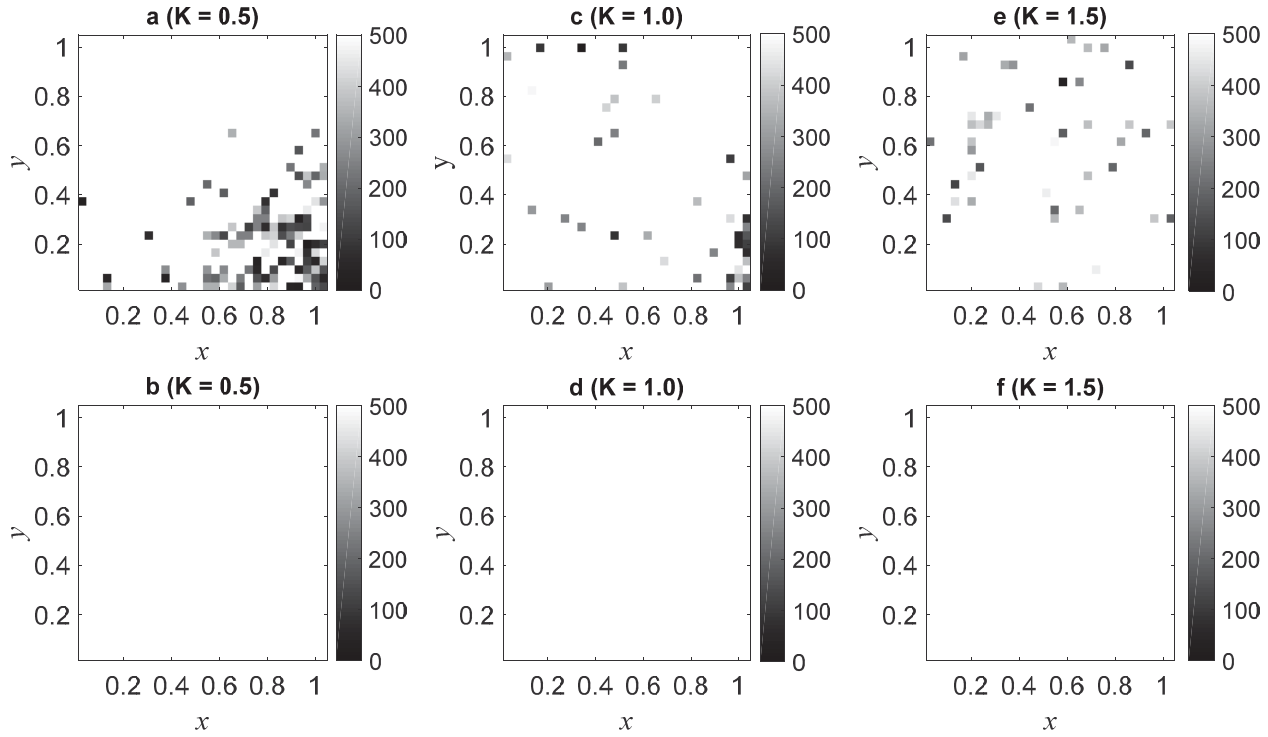

Fig. 4. Estimations of the start time of the periodic mode in the chaotic sequence obtained for different *K*

IV. Pseudo-random generation

The common way to construct a chaos-based stream cipher is the generation of a pseudo-random sequence to mask a plaintext. In 2014 Stoyanov and Kordov described the pseudo-random number generator (PRNG) based on a pair of two Chirikov standard maps with different *K* [12]. In the proposed scheme the floating-point numbers are transformed to a sequence of 0 and 1 using the comparison procedure and the Jabri shrinking rule. Patidar proposed a simpler generation scheme [13]. The pseudorandom bits are obtained by comparing two outputs of two maps in the following way:

$$f(x_1,x_2)=\begin{cases}1, x_1 \le x_2,\\ 0, x_1 > x_2.\end{cases}$$

The block diagram of single iteration of generation process is shown in Fig. 5.

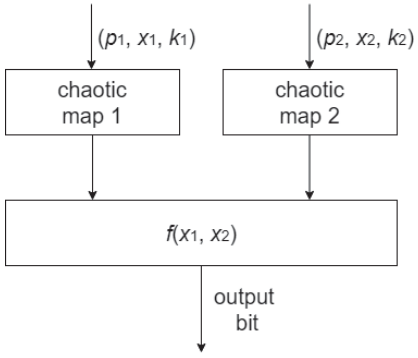

Fig. 5. The bit-generation scheme

Following Patidar, we considered PRNG based on two adaptive Chirikov maps. For both map the proposed perturbation mechanism was implemented. All computational experiments described in this section were carried out with *double* precision IEEE floating-point numbers.

A. Key space analysis

In paper [12] Stoyanov and Kordov do not discuss the size of the key space of the proposed PRNG. The considered generator was based on the Chirikov map with one nonlinearity parameters and two initial conditions. These values are represented using *double* data type with precision of 53 bits. Thus, the size of the key space is $2^{53} \times 2^{53} \times 2^{53}$. The generation algorithm based on the adaptive map possesses the same number of parameters and initial conditions. However, the symmetry coefficients used for perturbations in the proposed technique are also the part of the key. Thus, the size of the key space is $2^{53} \times 2^{53}$ times larger than for the generator based on the original Chirikov map. It is believed that a secure cryptosystem must have the key space larger than 2^{100} to be robust against brute-force attack [14]. Thus, the proposed approach meets this minimum criteria.

B. Statistical analysis

The common way to investigate PRNG is statistical testing. We used the NIST suite proposed by the Information Technology Laboratory in 2001 [15]. NIST tests define contingency measure of the binary sequences obtained by the investigated generator. Test bench consists of 15 tests. Each test calculates the statistics characterizing one of the properties of the set of generated sequences. Then, the probability p_{value} is calculated using the statistic value. The result is compared with

the level of the statistical significance α . If p_{value} exceeds α , then the test decision is positive.

Our experiment provided a set of 100 sequences of 10^6 bits each using the following initial numbers and parameters: $p_0 = 0.1,\ x_0 = 0.2,\ K_1 = 1500,\ K_2 = 2100,\ S_1 = 1,\ S_2 = 0.5$. To obtain each sequence we shifted the initial point 100 times to the machine epsilon. The level of significance α in our experiments was 0.01. The obtained results for the Stoyanov-Kordov PRNG and the proposed PRNG are presented in Table 1 and 2, respectively.

TABLE I. RESULTS OF NIST TESTING FOR PRNG BASED ON THE CHIRIKOV MAP

NIST Statistical test	P-value	Pass rate
Frequency	0.867692	99/100
Block frequency	0.224821	98/100
Runs	0.080519	100/100
Longest Run of Ones	0.851383	99/100
Binary Matrix Rank	0.867692	100/100
Spectral	0.779188	98/100
Non-overlapping Template Matching	0.213309	97/100
Overlapping Template Matching	0.699313	99/100
Universal Statistical Test	0.851383	99/100
Linear Complexity	0.534146	98/100
Serial Test 1	0.236810	100/100
Serial Test 2	0.080519	100/100
Approximate Entropy	0.236810	99/100
Cumulative Sums (forward)	0.383827	98/100
Cumulative Sums (backward)	0.181557	99/100
Random Excursions	0.719747	100/100
Random Excursions Variant	0.554420	98/100

TABLE II. RESULTS OF NIST TESTING FOR PRNG BASED ON THE ADAPTIVE CHIRIKOV MAP

NIST Statistical test	P-value	Pass rate
Frequency	0.534146	98/100
Block frequency	0.798139	100/100
Runs	0.145326	100/100
Longest Run of Ones	0.013569	100/100
Binary Matrix Rank	0.090936	98/100
Spectral	0.867692	99/100
Non-overlapping Template Matching	0.304126	99/100
Overlapping Template Matching	0.304126	99/100
Universal Statistical Test	0.759756	98/100
Linear Complexity	0.897763	98/100
Serial Test 1	0.574903	98/100
Serial Test 2	0.085587	100/100
Approximate Entropy	0.739918	99/100
Cumulative Sums (forward)	0.616305	98/100
Cumulative Sums (backward)	0.090936	98/100
Random Excursions	0.834308	97/100
Random Excursions Variant	0.304126	99/100

One can see that the investigated generator produces sequences with random properties. For PRNG based on the original Chirikov map the results of numerical studies were consistent with the experimental layouts presented in [12].

C. Correlation analysis

Correlation analysis of pseudo-random sequences allows to detect the relationship between elements of the dataset. It is known, that the sequences with a correlation coefficient less than 0.3 can be used for cryptographic purposes. We calculated the Pearson correlation coefficient for all pair of sequences generated in the previous experiments. The distributions of obtained values are shown in Fig. 6 and 7. As one can see, calculated values for both set of sequences do not exceed 0.015. According to the Chaddock scale, the obtained data correspond to the weak correlation relationship.

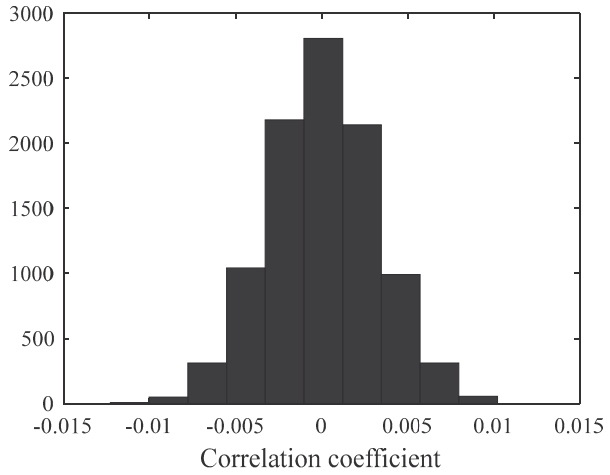

Fig. 6. The distribution of the Pearson correlation coefficient calculated for the sequences generated by the PRNG based on the Chirikov map

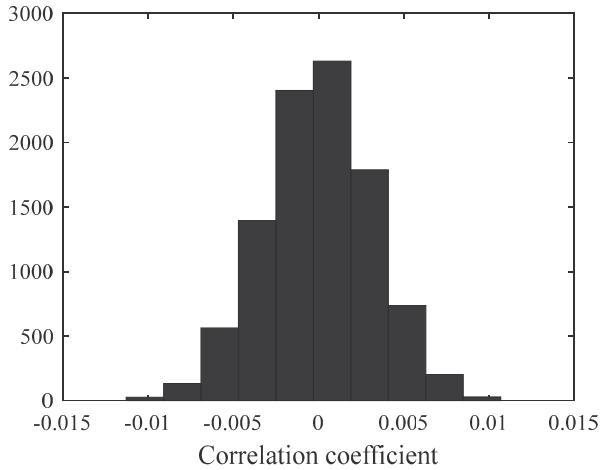

Fig. 7. The distribution of the Pearson correlation coefficient calculated for the sequences generated by the PRNG based on the adaptive Chirikov map

Thus, the perturbation of the symmetry coefficient extends the period of the generated sequence and keeps the statistical properties of the sequences close to the properties of random ones.

V. Conclusion

In this study, the application of the adaptive Chirikov map to pseudo-random generators was investigated. To overcome the problem of a short chaotic period in a fixed-point implementation, we proposed the technique for perturbing the symmetry coefficient of the map. The experimental results have shown that the perturbation of the adaptive maps according to the LSFR rule allows breaking cycles in calculations with 8-bit fractional precision. We implemented PRNG based on the pair of perturbed adaptive Chirikov maps and performed statistical and correlation analysis of generated sequences. The results have shown that the obtained sequences meet the criteria of the NIST statistical test suite and show correlation properties similar to the random sequences.

Thus, the obtained results can be used in chaos-based cryptography and security. Theoretically, chaotic encryption is faster than traditional approaches [4]. Therefore, the estimation of encryption speed of multimedia data is of interest. Moreover, it is necessary to study the possibility of various attacks including the reconstructing the phase space of the perturbed adaptive maps, since it is known that some chaotic maps are not able to resist such attack [16].

One of the possible directions in further studies can be a search for other applications of maps with adaptive symmetry, where this property can be effectively used. In addition, various techniques can be developed to implement the perturbation of the symmetry coefficient.

Acknowledgment

Artur I. Karimov was supported by grant of the President of Russian Federation, project MK-811.2019.1.

References

[1] F. Dachselt, W. Schwarz, “Chaos and cryptography”, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, Jan. 2001, pp. 1498-1509.

[2] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, Butusov, D. N., “Image encryption using finite-precision error”, *Chaos, Solitons & Fractals*, vol. 123, 2019, pp. 69-78.

[3] E. G. Nepomuceno, L. G. Nardo, J. Arias-Garcia, D. N. Butusov, A.V. Tutueva, “Image encryption based on the pseudo-orbits from 1D chaotic map” *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 29(6), 2019, 061101.

[4] C. Jeyamala, S.J. Thiruvengadam, “Ensemble of chaotic and naive approaches for performance enhancement in video encryption”, *The Scientific World Journal*, vol. 2015, article 458272, p. 11.

[5] K.J. Persohn, R.J. Povinelli, “Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation”, *Chaos, Solitons & Fractals*, vol. 45, Mar. 2012, pp. 238-245.

[6] H. Hu, Y. Deng, L. Liu, “Counteracting the dynamical degradation of digital chaos via hybrid control”, *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, Jun. 2014, pp. 1970-1984.

[7] G. Spenger and J. Keller, “Structural improvements of chaotic PRNG implementations”, *In Proc. 2016 11th International Conference for Internet Technology and Secured Transactions*, Dec. 2016, pp. 465-470.

[8] L. Merah, A. Ali-Pacha, N. Hadj-Said, H. Belkacem, “New and efficient method for extending cycle length of digital chaotic systems”, *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 43, Jul. 2019, pp. 259-268.

[9] B.V. Chirikov, *Research concerning the theory of non-linear resonance and stochasticity*, 1971.

[10] D.N. Butusov, A.I. Karimov, N.S. Pyko, S.A. Pyko, M.I. Bogachev, “Discrete chaotic maps obtained by symmetric integration”, *Physica A: Statistical Mechanics and its Applications*, vol. 509, Nov. 2018, pp. 955-970.

[11] A. I. Karimov, D. N. Butusov, V. G. Rybin and T. I. Karimov, “The study of the modified Chirikov map”, *In Proc. 2017 XX IEEE International Conference on Soft Computing and Measurements*, May. 2017, pp. 341-344.

[12] B. Stoyanov and K. Kordov, “A novel pseudorandom bit generator based on Chirikov standard map filtered with shrinking rule”, *Mathematical Problems in Engineering*, vol. 20, Jun. 2014.

[13] H. Ting, L. Gong, C. Ouyang, “An image encryption scheme combining chaos with cycle operation for DNA sequences”, *Nonlinear Dynamics*, vol. 87, Jan. 2017, pp. 51-66.

[14] V. Patidar, K. K. Sud, N. K. Pareek, “A pseudo random bit generator based on chaotic logistic map and its statistical testing”, *Informatica*, vol. 33(4), 2009.

[15] A. Rukhin et al., *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Booz-Allen and Hamilton Inc Mclean Va, 2001.

[16] J. Oravec, J. Turán, Ľ. Ovseník, T. Huszaník, “A Chaotic Image Encryption Algorithm Robust against Phase Space Reconstruction Attacks”, *Acta Polytechnica Hungarica*, vol. 16, no. 3, 2019, pp. 37–57.