

Информатика, вычислительная техника и управление

УДК 004.056.55

DOI: 10.30987/1999-8775-2019-2019-11-46-54

Д.Н. Бутусов, А.В. Тутуева, А.И. Каримов, Т.И. Каримов

**МОДЕЛИ ХАОТИЧЕСКИХ СИСТЕМ С УПРАВЛЯЕМОЙ СИММЕТРИЕЙ
В ПОТОКОВОМ ШИФРОВАНИИ**

Проведено исследование с целью повышения эффективности шифрования на основе хаотических систем за счет применения моделей с управляемым коэффициентом симметрии. В качестве методов исследования использованы вычислительный эксперимент, методы статистического анализа и теории численных методов интегрирования. Получены

новые модели хаотических систем с управляемой симметрией и способ увеличения периода хаотической последовательности путем возмущения коэффициента симметрии.

Ключевые слова: хаотическая система, мемристор, шифрование, управляемая симметрия, полунявное интегрирование.

D.N. Butusov, A.V. Tutueva, A.I. Karimov, T.I. Karimov

**MODELS OF RANDOM SYSTEMS WITH CONTROLLED SYMMETRY IN STREAM
ENCRYPTION**

Information safety plays an important role in modern technologies. A stream encryption is one of the common means for information safety support. The sequences with pseudo-random characteristics are often required in the algorithms of stream enciphering. Random systems are recently used as a source of pseudo-random numbers with desired statistical properties. A small length of a sequence period is one of the known problems of the generators of pseudo-random numbers based on chaos realized with a small length of a digit grid. The disturbance of a path or a parameter of random system nonlinearity is one of possible solutions of a short period problem. In this paper there is considered a new approach to the increase of a period length through the change of a symmetry factor in the random model of a memristive circuit. The approach offered is

based on switching two values of the symmetry factor in accordance with the output of a shear register with the linear feedback. To confirm the effectiveness of the disturbance circuit described the lengths of a period for the disturbed and original model of the memristive system are estimated. The properties of the output sequences caused by a generator on the basis of the model with controlled symmetry are confirmed by the results of the correlation analysis and NIST statistical testing.

The results obtained can be used in cryptographic applications and also at the designing of safe communication systems.

Key words: random system, memristor, enciphering, controlled symmetry, semi-non-evident integration.

Введение

Хаотическое шифрование - одна из перспективных областей современной криптографии. Эргодичность, топологическое смешивание и высокая чувствительность к начальным условиям и изменениям параметров хаотических систем схожи с традиционно рассматриваемыми процессами перемешивания и рассеивания в традиционных алгоритмах криптографии [1-3]. Использование хаотических систем для генерации псевдослучайных последовательностей (ПСП) в потоковых шифрах обеспечивает высокую скорость шифрования. Поэтому криптографические системы на основе детерминированного хаоса

представляют интерес с точки зрения безопасной обработки и передачи мультимедийных данных [4].

Одной из ключевых проблем систем хаотического шифрования, реализуемых на ЭВМ с ограниченной точностью представления данных, является малая длина периода квазихаотической последовательности. В работе [5] К. Персон представил результаты моделирования логистического отображения с использованием арифметики с фиксированной запятой с четырьмя битами для описания дробной части. Автором было показано, что вне зависимости от выбора начальных условий значения

начинают повторяться с периодом, равным трем, после всего двух итераций. Одним из перспективных методов увеличения периода квазихаотической последовательности является использование алгоритмов возмущения орбиты или параметра хаотической системы [6; 7]. В частности, в работе [6] было показано, что переключение между двумя значениями параметра логистического отображения значительно увеличивает период квазихаотической последовательности. Стоит отметить, что при возмущении параметра нелинейности системы необходимо отслеживать текущий режим колебаний, определяя его тип - гармонический или хаотический.

В настоящей работе мы предлагаем собственное решение обозначенной выше проблемы путем использования моделей хаотических систем с новым управляемым параметром, называемым коэффициентом симметрии. Изменение коэффициента симметрии осуществляет аффинное преобразование фазового пространства, поэтому его возмущение не влияет на нелинейные свойства системы. Помимо этого, коэффициент симметрии может являться частью ключа для потоковых шифров на основе хаоса. Таким образом, возможно потенциальное повышение криптографической стойкости схем шифрования на основе хаоса.

Модели хаотических систем с управляемой симметрией

Идея дискретных моделей хаотических систем с управляемой симметрией является развитием концепции симметричных хаотических отображений, описанных ранее в работах Д.Н. Бутусова и А.И. Каримова [8; 9]. Отображения Чирикова и Хенона, демонстрирующие симметрию в фазовом пространстве, были получены путем интегрирования гамильтоновых систем. Симметрия достигается за

счет применения композиции двух сопряженных полуявных методов Эйлера - Кромера на интервалах $[t_n; t_{n+0.5h}]$ и $[t_{n+0.5h}; t_{n+h}]$ соответственно, где h - шаг интегрирования. При изменении момента интегрирования с 0.5 на коэффициент симметрии S (рис. 1) приобретает возможность управления поворотом в фазовом пространстве.

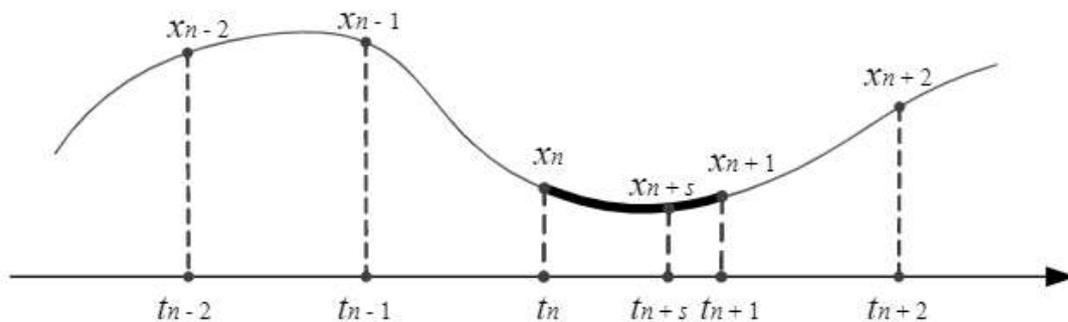


Рис. 1. Геометрическая интерпретация управления симметрией

Например, для хорошо изученного отображения Чирикова [10], устанавливающего взаимосвязь между импульсом p и координатой x как

$$p_{n+1} = p_n + K \sin x_n,$$

$$x_{n+1} = x_n + p_{n+1},$$

симметричная версия, имеющая вид

$$p_{n+0.5} = p_n + 0.5K \sin x_n,$$

$$x_{n+1} = x_n + p_{n+0.5},$$

$$p_{n+1} = p_{n+0.5} - 0.5K \sin x_{n+1},$$

может быть преобразована в модель с управляемой симметрией следующим образом:

$$p_{n+s} = p_n + SK \sin x_n,$$

$$x_{n+1} = x_n + p_{n+s}, \quad (1)$$

$$p_{n+1} = p_{n+s} - (1-S)K \sin x_{n+1}.$$

Фазовые портреты отображения (1) при разных значениях коэффициента симметрии представлены на рис. 2.

Аналогично дискретным хаотическим отображениям с управляемой сим-

метрией могут быть получены адаптивно-симметричные модели непрерывных систем. Рассмотрим систему обыкновенных дифференциальных уравнений (ОДУ), описывающих динамику цепи с мемристором - нелинейным элементом, изменяющим свое сопротивление в зависимости от протекающего через него заряда [11]:

$$\begin{cases} \frac{dx_1}{d\tau} = x_2; \\ \frac{dx_2}{d\tau} = -\delta x_1 - \beta(x_3^2 - 1)x_2; \\ \frac{dx_3}{d\tau} = -x_2 - \alpha x_3 + \gamma x_2 x_3. \end{cases} \quad (2)$$

Хаотический режим в системе (2) наблюдается при $\alpha=0.6$, $\beta=0.5$, $\gamma=1$, $\delta=1/3$. Применение мемристивных систем в потоковых шифрах представляет особый интерес, поскольку в отличие от многих других систем с хаотическим поведением такие системы подразумевают теоретическую возможность реализации генератора истинно случайных чисел [12] на перспективной элементной базе.

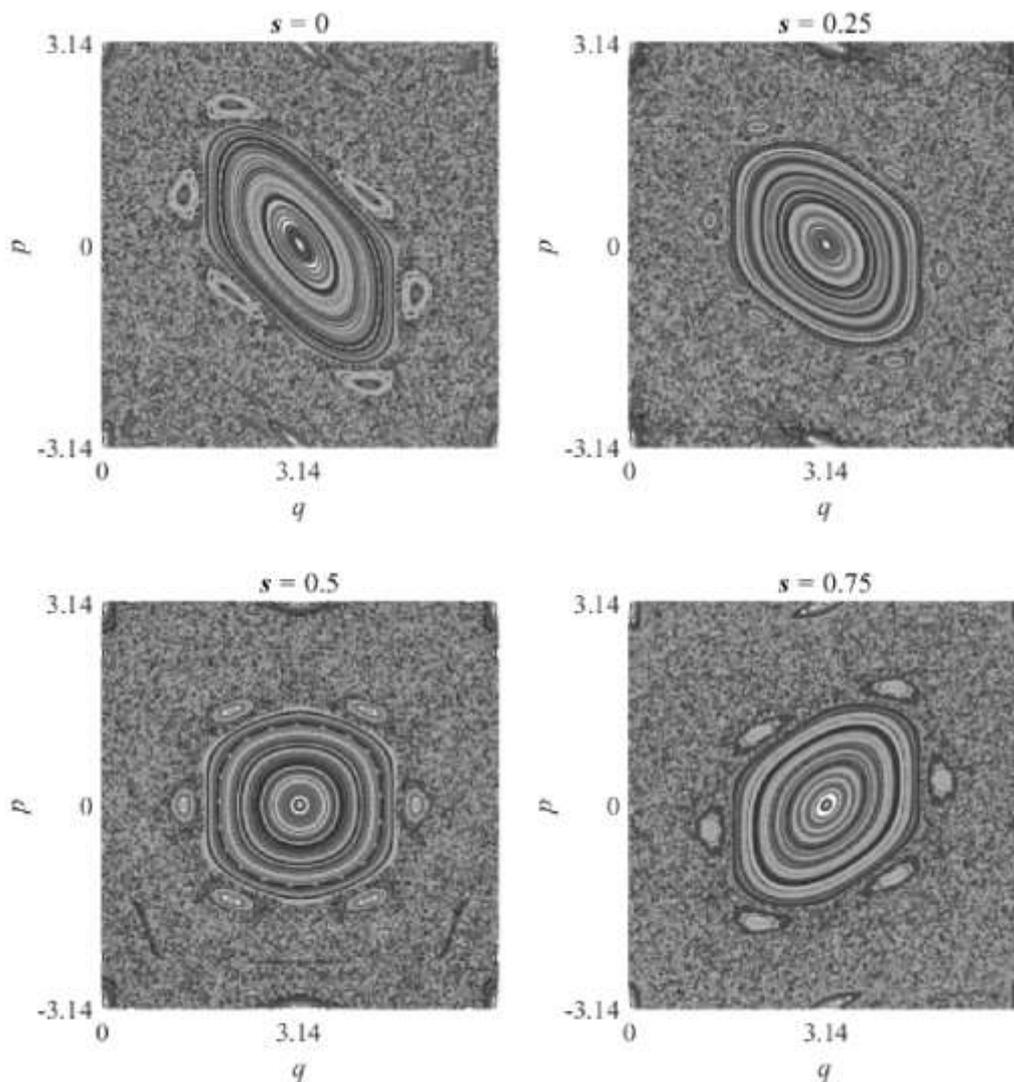


Рис. 2. Фазовые портреты отображения Чирикова с управляемой симметрией при разных S

От системы ОДУ (2) перейдем к конечно-разностной схеме, полученной пу-

тем применения полуявного метода интегрирования [13]:

$$\begin{aligned}
 x_{n+0.5} &= x_n + 0.5hy_n; \\
 y_{n+0.5} &= \frac{y_n - 0.5hx_{n+0.5}\delta}{1 + 0.5h\beta(z_n^2 - 1)}; \\
 z_{n+0.5} &= \frac{z_n - 0.5hy_{n+0.5}}{1 + 0.5h(\alpha - \gamma y_{n+0.5})}; \\
 z_{n+1} &= z_{n+0.5} + 0.5h(-y_{n+0.5} - \alpha z_{n+0.5} + \gamma y_{n+0.5} z_{n+0.5}); \\
 y_{n+1} &= y_{n+0.5} + 0.5h(-\delta x_{n+0.5} - \beta y_{n+0.5}(z_{n+1}^2 - 1)); \\
 x_{n+1} &= x_{n+0.5} + 0.5hy_{n+1}.
 \end{aligned} \tag{3}$$

Чтобы получить модель с управляемой симметрией, заменим коэффициент 0.5 в (3) на S , как ранее в случае дискрет-

ного отображения Чирикова. Итоговая модель системы примет вид

$$\begin{aligned}
 x_{n+S} &= x_n + Shy_n; \\
 y_{n+S} &= \frac{y_n - Shx_{n+S}\delta}{1 + Sh\beta(z_n^2 - 1)}; \\
 z_{n+S} &= \frac{z_n - Shy_{n+S}}{1 + Sh(\alpha - \gamma y_{n+S})}; \\
 z_{n+1} &= z_{n+S} + (1-S)h(-y_{n+S} - \alpha z_{n+S} + \gamma y_{n+S} z_{n+S}); \\
 y_{n+1} &= y_{n+S} + (1-S)h(-\delta x_{n+S} - \beta y_{n+S}(z_{n+1}^2 - 1)); \\
 x_{n+1} &= x_{n+S} + (1-S)hy_{n+1}.
 \end{aligned} \tag{4}$$

Возмущение коэффициента симметрии не влияет на нелинейный характер процесса, однако позволяет эффективно

избегать наступления периодического режима аналогично изменению параметра нелинейности.

Алгоритм возмущения коэффициента симметрии

Наиболее простая схема возмущения параметра нелинейности была описана Г. Спенгером в работе [6]. Предложенный им способ основан на переключении между двумя значениями параметра каждые N итераций. Хаотичность системы подразумевает, что малое изменение значения параметра приводит к значительному изменению поведения системы. Подход Спенгера показывает хорошие результаты при вычислениях с плавающей запятой. Однако при использовании типа данных с фиксированной запятой и малым количеством бит для представления дробной части хаотическая последовательность может стать периодичной еще до наступления N -й итерации. Поэтому в настоящей статье предлагается модифицировать этот подход

и использовать его для возмущения коэффициента симметрии, которое можно производить гораздо чаще за счет минимального влияния симметрии на хаотичность решения.

Пусть S_1 и S_2 - два значения коэффициента симметрии. Тогда возмущение хаотической системы с управляемой симметрией выполняется путем переключения коэффициента между двумя значениями S_1 и S_2 . Для определения момента переключения используется регистр сдвига с линейной обратной связью (РСЛОС). Значение S_1 соответствует нулевому биту на выходе РСЛОС, а S_2 - единичному. Предложенная схема возмущения коэффициента симметрии с РСЛОС, который задается примитивным многочленом $y^8 + y^6 + y^5 + y^4 + 1$, представлена на рис. 3.

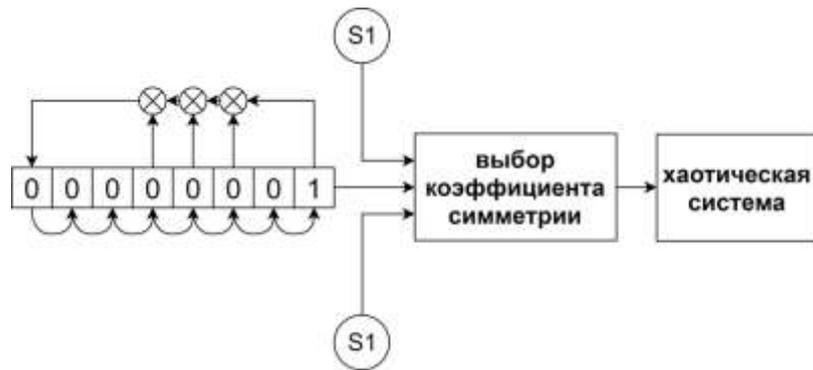


Рис. 3. Схема возмущения коэффициента симметрии модели хаотической системы

Рассмотрим применение предложенного подхода к мемристивной системе (2). Для оценки длины периода получаемой последовательности используем 16-битный тип данных с фиксированной точкой, где по 8 бит отводится на описание дробной и целой частей. Период оценим при моделировании системы с использованием

симметричной конечно-разностной схемы (3), а также схемы с управляемой симметрией (4) при начальных условиях $y_0 = 0$, $x_0 \in [0.0234375; 1]$ и $z_0 \in [0.0234375; 1]$. Для каждой пары начальных условий выполнялось моделирование на временном интервале 500 с с разными значениями α .

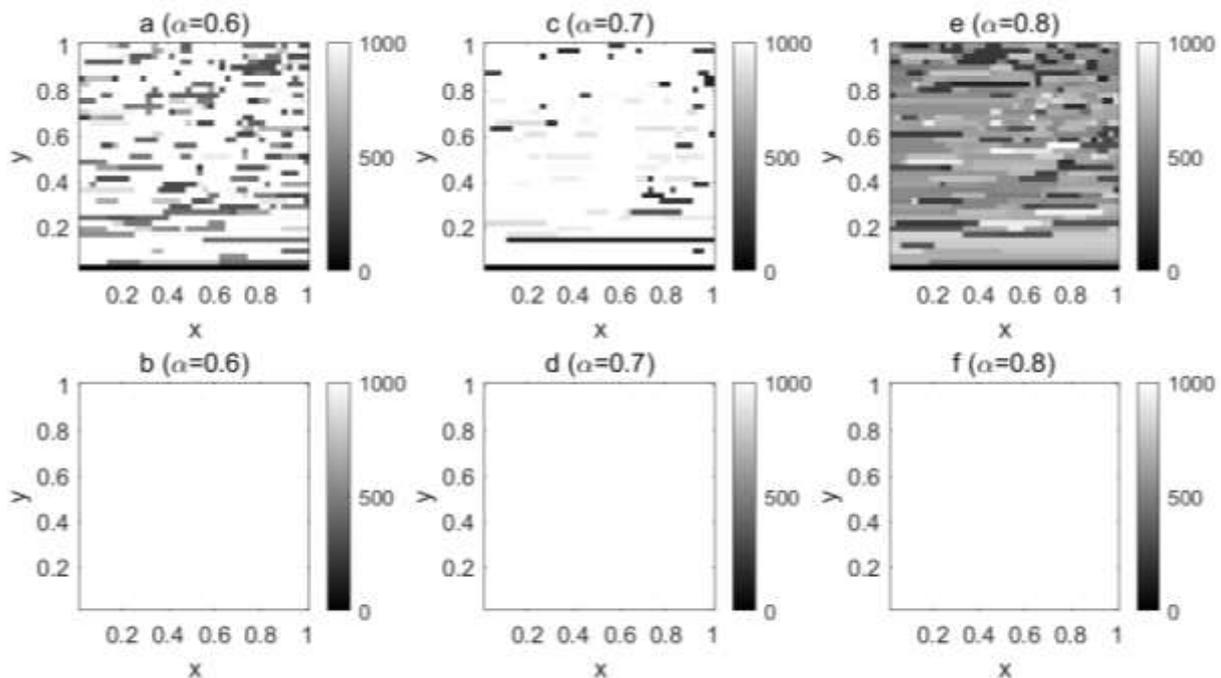


Рис. 4. Оценки времени начала периодического режима хаотических последовательностей, полученных для разных значений параметра нелинейности

Полученные результаты показаны на рис. 4. Белый цвет соответствует максимальному периоду, т.е. в этом случае каждое значение последовательности

встречалось ровно один раз. Как можно увидеть, предложенный способ возмущения решения позволяет увеличить период хаотической последовательности.

Генерация псевдслучайных последовательностей на основе моделей с управляемой симметрией

Одним из распространенных способов потокового шифрования является гаммирование - метод, заключающийся в

побитовом сложении по модулю 2 последовательности псевдслучайных чисел с открытым текстом. В 2014 г.

М. Француа и др. описали генератор ПСП на основе хаотических систем [14]. В предложенной схеме генерации из каждого числа с плавающей запятой извлекаются младшие 32 бита мантииссы. Полученные биты конкатенируются и образуют искомую последовательность.

Рассмотрим генератор ПСП, реализующий такой способ получения бит и использующий разработанный нами способ возмущения коэффициента симметрии. Для оценки генератора проведем статистический анализ генерируемых последовательностей.

Традиционным способом анализа генераторов ПСП является тестирование последовательностей с использованием пакетов статистических тестов. В настоящем исследовании использовались 15 статистических тестов NIST, разработанные в 2001 г. [15]. Пакет NIST позволяет определить меру случайности двоичных последовательностей, полученных исследуемым генератором.

Каждый тест вычисляет статистику, характеризующую одно из свойств набора сгенерированных последовательностей. Затем с использованием полученного значения статистики вычисляется вероятность $pvalue$. Результат сравнивается с уровнем статистической значимости α . Если $pvalue$ превышает α , то тест считается пройденным.

В настоящем исследовании рассматривался набор из 100 последовательностей длиной 10^6 бит каждая, которые были получены при $x_0 = z_0 = 0.492188$, $y_0 = 0$, $\alpha = 0.6$, $\beta = 0.5$, $\gamma = 1$, $\delta = 1/3$. Для получения каждой последовательности начальная точка сдвигалась 100 раз на величину машинного эпсилон. Доверительный уровень в проведенных экспериментах был равен 0.01. Полученные результаты представлены в таблице. Можно увидеть, что исследуемый генератор порождает последовательности с характеристиками случайных.

Таблица

Результаты статистического тестирования NIST

Статистический тест NIST	$pvalue$	Последовательности, прошедшие тест
Частотный побитовый тест	0.000001	98/100
Частотный блочный тест	0.071177	98/100
Тест на последовательность одинаковых битов	0.000883	100/100
Тест на самую длинную последовательность единиц в блоке	0.004629	100/100
Тест рангов бинарных матриц	0.455937	100/100
Спектральный тест	0.289667	99/100
Тест на совпадение неперекрывающихся шаблонов	0.026948	100/100
Тест на совпадение перекрывающихся шаблонов	0.383827	99/100
Универсальный статистический тест Маурера	0.080519	100/100
Тест на линейную сложность	0.350485	99/100
Тест на периодичность 1	0.006661	100/100
Тест на периодичность 2	0.001296	100/100
Тест приближительной энтропии	0.090936	100/100
Тест кумулятивных сумм (прямой)	0.000001	97/100
Тест кумулятивных сумм (обратный)	0.000002	98/100
Тест на произвольные отклонения	0.419021	100/100
Другой тест на произвольные отклонения	0.779188	99/100

Другим распространенным способом исследования генераторов ПСП является корреляционный анализ, позволяющий обнаружить степень взаимосвязи между элементами набора данных. Известно, что последовательности с коэффициентом корреляции, меньшим 0.3, могут быть

использованы для криптографических целей. Для всех пар последовательностей, рассмотренных в предыдущем эксперименте, был рассчитан коэффициент корреляции Пирсона. Распределение полученных значений показано на рис. 5.

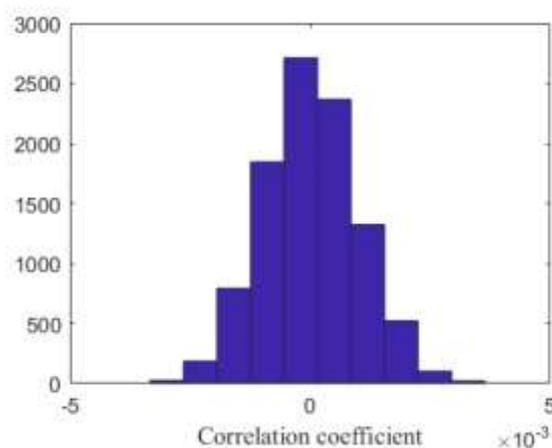


Рис. 5. Распределение коэффициента корреляции Пирсона для последовательностей, полученных генератором ПСП на основе модели хаотической системы с управляемой симметрией

Как можно увидеть, вычисленные значения для полученного набора последовательностей по модулю не превышают 0.005, что соответствует слабой корреляционной связи.

Заключение

В статье исследовалось применение модели хаотической системы с управляемой симметрией для генерации гамм в потоковых шифрах. Был предложен алгоритм возмущения коэффициента симметрии для продления периода хаотической последовательности. Предложенный метод основан на переключении двух значений коэффициента симметрии в соответствии с выходом РСЛОС. Результаты экспериментов показали, что применение такого подхода позволяет увеличивать период последовательности при вычислениях с числами с фиксированной запятой с 8-битной дробной частью. Для последовательностей, порожденных генератором ПСП на основе полученной модели с управляемой симметрией, был выполнен статистический анализ. Экспериментально показано, что сгенерированные последовательности удовлетворяют критериям пакета статистиче-

Таким образом, возмущение коэффициента симметрии расширяет период генерируемой последовательности и сохраняет свойства последовательностей близкими к свойствам случайных.

ских тестов NIST и показывают корреляционные свойства, близкие к случайным последовательностям.

Полученные результаты могут быть использованы в хаотической криптографии для разработки новых методов шифрования данных. Теоретически хаотическое шифрование может быть вычислительно эффективнее, чем традиционные подходы [4], поэтому особый интерес представляет оценка скорости шифрования мультимедийных данных. Кроме того, одним из направлений дальнейших исследований является изучение возможности проведения различных атак, включая реконструкцию фазового пространства, поскольку известно, что некоторые системы шифрования на основе хаотических систем не способны противостоять такой атаке [16].

Д.Н. Бутусов, А.В. Тутуева, Т.И. Каримов получили поддержку Российского фонда фундаментальных исследований в рамках проекта 19-07-00496\19 «Основы исследовательского проектирования

мемристивных систем». А.И. Каримов получил финансирование по гранту Президента для молодых ученых – кандидатов наук МК-811.2019.1.

СПИСОК ЛИТЕРАТУРЫ

1. Пермяков, В.Б. Технологические машины и комплексы в дорожном строительстве (производственная и техническая эксплуатация) / В.Б. Пермяков, С.В. Мельник, В.И. Иванов [и др.]; под ред. В.Б. Пермякова. - М.: БАСТЕТ, 2014. - 752 с.
2. Бурый, Г.Г. Грейфер сферический / Г.Г. Бурый, И.К. Потеряев // Мир транспорта и технологических машин. - 2017. - № 2. - С. 47-50.
3. Plonecki, L. A concept of digital control system to assist the operator of hydraulic excavators / L. Plonecki, W. Trampczynski, J. Cendrowicz // Automation in construction. - 1998. - № 5. - P. 401-411.
4. Зеленин, А.Н. Машины для земляных работ / А.Н. Зеленин, В.И. Баловнев, И.П. Керов. - М.: Машиностроение, 1975. - 424 с.
5. Landberg, L. Excavators combine compactness and power / L. Landberg // Construction equipment. - 2003. - № 8. - P. 58-59.
6. Павлов, В.П. Рекомендации по выбору параметров экскаваторных ковшей / В.П. Павлов, А.Н. Абрамов // Транспортное строительство. - 1984. - № 7. - С. 35-36.
7. Пат. 2656286 Российская Федерация, МПК E02F 3/28. Ковш экскаватора сферический / Бурый Г.Г.; заявитель и патентообладатель Бурый Г.Г.
8. Заявка 2018114378/20(022485) Российская Федерация, МПК E02F 3/40. Способ копания одноковшовым гидравлическим экскаватором и одноковшовый гидравлический экскаватор / Бурый Г.Г., Щербаков В.С.; заявитель Сибирский государственный автомобильно-дорожный университет (СибАДИ).
9. Sinclair, R. Hydraulic Excavators: Quarrying & Mining Applications / R. Sinclair. - London: Sinclair Publishing, 2011. - 388 p.
10. Ветров, Ю.А. Резание грунтов землеройными машинами / Ю.А. Ветров. - М.: Машиностроение, 1971. - 357 с.
11. Баловнев, В.И. Моделирование процессов взаимодействия со средой рабочих органов дорожно-строительных машин / В.И. Баловнев. - М.: Высш. шк., 1981. - 335 с.
12. Demishcan, V. Experimental researches of the process of enterworking of the operational parts of excavators with soil / V. Demishcan // Вестник Харьковского национального автомобильно-дорожного университета. - 2008. - № 43. - С. 115-118.
13. Тарасов, В.Н. Механика копания грунтов, основанная на теории предельных касательных напряжений / В.Н. Тарасов, М.В. Коваленко // Строительные и дорожные машины. - 2003. - № 7. - С. 38-43.
14. Кузнецова, В.Н. Обеспечение энергоэффективности разработки грунта за счет оптимизации углов позиционирования рабочего оборудования экскаватора / В.Н. Кузнецова, В.В. Савинкин // Строительные и дорожные машины. - 2015. - № 3. - С. 44-47.
1. Politsansky, R.L. System for data transfer with enciphering by random sequences / R.L. Politsansky [et al.] // *Technology and Design in Electronic Equipment*. - 2014.
2. Ponomarenko, V.I. Confidentiality estimate of information transfer system based on random generator with delay and switchable period of delay / V.I. Ponomarenko [et al.] // *Information-Control Systems*. - 2019. - No.4. - pp. 54-61.
3. Kaliyanov, G.N. Information enciphering using random solutions of deterministic equations / G.N. Kaliyanov, E.V. Kaliyanov // *Letters to ZhTF*. - 2005. - Vol. 31. - No. 24. - pp. 45.
4. Degtyaryov, S.A. Enciphering method based on random method with controlled path / S.A. Degtyaryov, V.M. Dovgal, I.S. Zakharov // *Telecommunications*. - 2008. - No.7. - pp. 29-31.
5. Persohn, K.J. Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation / K.J. Persohn, R.J. Povinelli // *Chaos, Solitons & Fractals*. - 2012. - Vol. 45. - P. 238-245.
6. Spenger, G. Structural improvements of chaotic PRNG implementations / G. Spenger, J. Keller // 11th International Conference for Internet Technology and Secured Transactions. - 2016. - P. 465-470.

7. Kogay, G.D. Cryptographic systems for deterministic chaos control / G.D. Kogay [et al.] // *International Journal of Applied and Fundamental Investigations*. – 2014. – No.1-2. – pp. 287-290.
8. Butusov, D.N. Discrete chaotic maps obtained by symmetric integration / D.N. Butusov, A.I. Karimov, N.S. Pyko, S.A. Pyko, M.I. Bogachev // *Physica A: Statistical Mechanics and its Applications*. – 2018. – Vol. 509. – P. 955-970.
9. Karimov, A.I. Investigation of Chirikov modified representation / A.I. Karimov [et al.] // *Inter. Conf. on Soft Computations and Measurements*. – Uliyanov (Lenin)SETU of S-Pb. “LETI”, 2017. – Vol.1. – pp. 400-403.
10. Chirikov, B.V. Research concerning the theory of non-linear resonance and stochasticity / B.V. Chirikov. – 1971.
11. Butusov, D.N. Numerical analysis of memristor-based circuits with semi-implicit methods / D.N. Butusov, V.Y. Ostrovskii, D.O. Pesterev // *Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus)*. – IEEE, 2017. – P. 271-276.
12. Jiang, H. A novel true random number generator based on a stochastic diffusive memristor / H. Jiang [et al.] // *Nature communications*. – 2017. – T. 8. – № 1. – P. 882.
13. Butusov, D.N. Extrapolation Semi-implicit ODE solvers with adaptive timestep / D.N. Butusov, A.V. Tutueva, E.S. Homitskaya // *XIX International Conference on Soft Computing and Measurements (SCM)*. – IEEE, 2016. – P. 137-140.
14. Francois, M. A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic / M. Francois, D. Defour, C. Negre. – 2014.
15. Poty, A. *Statistical Testing of Generators of Random and Pseudo-random Numbers Using NIS STS Statistical Test Set* / A.Poty, S. Orlova, T. Grinenko. – 2001.
16. Kuznetsov, S.P. *Dynamic Chaos* / S.P. Kuznetsov // *Proceedings of Higher Education Institutions. Applied Nonlinear Dynamics*. – 2002. – Vol. 10. – No.1-2. – pp. 189-191.

Ссылка для цитирования:

Бутусов, Д.Н. Модели хаотических систем с управляемой симметрией в потоковом шифровании / Д.Н. Бутусов, А.В. Тутуева, А.И. Каримов, Т.И. Каримов // *Вестник Брянского государственного технического университета*. – 2019. – № 11. – С. 46–54. – DOI: 10.30987/1999-8775-2019-2019-11-46-54.

Статья поступила в редакцию 30.10.19.

Рецензент: к.т.н., доцент Брянского государственного технического университета,
член редсовета журнала «Вестник БГТУ»

Рытов М.Ю.

Статья принята к публикации 11. 11. 19.

Сведения об авторах:

Бутусов Денис Николаевич, к.т.н., доцент кафедры систем автоматизированного проектирования Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), e-mail: dnbutusov@etu.ru.

Тутуева Александра Вадимовна, ассистент кафедры систем автоматизированного проектирования Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), e-mail: avtutueva@etu.ru.

Butusov Denis Nikolaevich, Can. Sc. Tech., Assistant Prof. of the Dep. “Computer Aided Design”, Uliyanov State Electrotechnical University “LETI” of Saint-Petersburg, e-mail: dnbutusov@etu.ru.

Tutueva Alexandra Vadimovna, Assistant of the Dep. “Computer Aided Design”, Uliyanov State Electrotechnical University “LETI” of Saint-Petersburg, e-mail: avtutueva@etu.ru.

Каримов Артур Искандарович, к.т.н., доцент кафедры систем автоматизированного проектирования Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), e-mail: aikarimov@etu.ru.

Каримов Тимур Искандарович, к.т.н., ст. преподаватель кафедры систем автоматизированного проектирования Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), e-mail: tikarimov@etu.ru.

Karimov Arthur Iskanderovich, Assistant Prof. of the Dep. “Computer Aided Design”, Uliyanov State Electrotechnical University “LETI” of Saint-Petersburg, e-mail: aikarimov@etu.ru.

Karimov Timur Iskanderovich, Can. Sc. Tech., Senior Lecturer of the Dep. “Computer Aided Design”, Uliyanov State Electrotechnical University “LETI” of Saint-Petersburg, e-mail: tikarimov@etu.ru.