Статистические характеристики генераторов псевдослучайных сигналов на основе систем Лоренца, Чуа и Дмитриева-Кислова, реализованных над конечным полем Галуа

С.С. Логинов, М.Ю. Зуев

Казанский национальный исследовательский технический университет им. А.Н. Туполева

Аннотация: Рассмотрены статистические характеристики и результаты тестов FIPS 140-2 нового класса генераторов псевдослучайных сигналов, построенных на основе модифицированных систем Лоренца, Чуа и Дмитриева-Кислова над конечным полем Галуа. Получены оценки уровней боковых лепестков корреляционных функций сигналов, а также гистограммы распределений вероятностей формируемых чисел. Получены оценки соответствия двоичных последовательностей, формируемых на основе систем требованиям теста FIPS 140-2 при вариации параметров системы. Результаты работы могут быть использованы при построении систем связи с широкополосными сигналами, моделирования и криптографии.
Ключевые слова: динамический хаос, радиоэлектронная динамическая система, статистическая характеристика

I. ВВЕДЕНИЕ

Многие физические явления можно в той или иной мере описать как хаотические процессы. Динамические системы с хаотическим поведением используются в радиотехнике и телекоммуникациях как для описания радиоэлектронных схем [1], так и в качестве новых носителей информации [2]. Нелинейные радиоэлектронные устройства и системы характеризуются большим разнообразием регулярных и хаотических мод. Поэтому одним из перспективных приложений нелинейных систем с хаотической динамикой является формирование псевдослучайных сигналов с требуемыми статистическими характеристиками в системах связи, моделирования и криптографии. В частности, генераторы хаоса используются для создания последовательностей псевдослучайных чисел. В радиотехнике хаос может применяться для модулирования несущей при создании широкополосных сигналов цифровыми методами (на программируемых логических интегральных схемах или процессорах).

В отличие от шума, который является случайным процессом, динамический хаос описывается детерминированными системами уравнений. Хаотические системы чувствительны к начальным условиям, и малейшие их изменения могут привести к колоссальным различиям.

В настоящее время достаточно широко исследованы нелинейные динамические системы Лоренца, Чуа, системы фазовой автоподстройки частоты, системы связанных генераторов, кольцевые автоколебательные системы Дмитриева-Кислова, генераторы с инерционной нелинейностью Анищенко-Астахова, системы на основе элементов задержки с сумматорами по модулю, нелинейные отображения Бернулли, Хенона, Лози с хаотической динамикой [3,4].

Формирование псевдослучайных сигналов с требуемыми в системах связи, моделирования и криптографии статистическими характеристиками является наиболее интересным и важным аспектом применения хаотических систем.

Целью данной работы является синтез новых генераторов псевдослучайных сигналов на основе систем Лоренца, Чуа и Дмитриева-Кислова, а также оценка статистических характеристик формируемых ими последовательностей требованиям, предъявляемым к генераторам случайных и псевдослучайных последовательностей и требованиям тестов FIPS-140-2.

II. МЕТОДЫ И ОГРАНИЧЕНИЯ

В процессе практической реализации систем на элементах программируемой логики важным является использование более простых форматов представления данных с наименьшим возможным числом разрядов. Это могут быть форматы с фиксированной запятой, а также целые числа. В последнем случае система, представленная вместо арифметики с плавающей запятой в целочисленном формате, полностью теряет связь с исходной динамической системой. На основе некоторой первоначальной системы формируется новая система, в которой все операции выполняются над числами в полях Галуа соответствующей размерности. В данной работе при представлении чисел в формате unsigned integer 16 и замене арифметических операций на операции над полем Галуа $GF(2^{16})$.

В качестве первой исходной динамической системы, которая подвергается модификации, в работе была выбрана динамическая система Лоренца [3]:

$$\begin{cases} X_{i+1} = X_i + t(\sigma \cdot X_i + \sigma \cdot Y_i), \\ Y_{i+1} = Y_i + t(r \cdot X_i + Y_i + X_i \cdot Z_i), \\ Z_{i+1} = Z_i + t(b \cdot Z_i + X_i \cdot Y_i); \end{cases} \quad (1)$$

где t – шаг интегрирования; r, σ, b – параметры системы, а все операции в уравнениях производятся над полем Галуа.

Вторая исследуемая система была получена на основе исходной системы Чуа

$$\begin{cases} X_{i+1} = X_i + t(a(h(X_i) + Y_i)), \\ Y_{i+1} = Y_i + t(X_i + Y_i + Z_i), \\ Z_{i+1} = Z_i + t(b \cdot Y_i); \end{cases} \quad (2)$$

где t – шаг интегрирования; a, b - параметры системы, а все операции в уравнениях производятся также над полем Галуа; $h(X_i)$- определяет

характеристику нелинейности используемой в системе. При исследовании нелинейность $h(X_i)$ имела характеристику, состоящую из трех участков:

$$h(X_i)=\begin{cases} c1\cdot X_i + c1 + c2, & X_i \le N/2 \\ c1\cdot X_i + c2, & X_i > N \\ c1\cdot X_i; & N/2 < X_i \le N \end{cases} \quad (3)$$

где $c1$, $c2$, и N - параметры системы.

Третья система была получена на основе системы Дмитриева-Кислова

$$\begin{cases} X_{i+1} = X_i + (t/T)(X_i + M\cdot Z_i \cdot 2^{Z_i}), \\ Y_{i+1} = Y_i + t(X_i + Z_i \cdot Y_i), \\ Z_{i+1} = Z_i + t(X_i \cdot Y_i + Z_i \cdot Q); \end{cases} \quad (4)$$

где t – шаг интегрирования; T, M, Q - параметры системы.

В работе анализируются фазовые портреты, гистограммы формируемых последовательностей, авто- и взаимно-корреляционные функции сигналов и их соответствие тестам FIPS 140-2.

Равномерность распределения оценивается по критерию χ^2 степени согласованности теоретического и статистического распределения

$$\chi^2 = \sum_{i=1}^{n} \frac{(m_i - np_i)^2}{np_i} \quad (5)$$

Важнейшими характеристиками бинарных хаотических последовательностей являются их автокорреляционные функции (АКФ), взаимно-корреляционные функции (ВКФ).

Автокорреляционные функции сигналов являются характеристиками, показывающими наличие внутренних связей в них и имеют первостепенное значение при практическом применении последовательностей псевдослучайных чисел для передачи информации. Поэтому в работе акцент делается на оценке апериодических автокорреляционных функций (6) и взаимнокорреляционных функций (7) полученных кодовых последовательностей.

$$\rho(m) = \frac{1}{\|a\|^2} \sum_{i=0}^{N-1} a_i a_{i-m}^* \qquad (6)$$

$$\rho_{a,kl}(m) = \begin{cases} \frac{1}{\|a_k\| \cdot \|a_l\|} \sum_{i=0}^{N-1} a_{k,i} a_{l,i-m}^*, & m \geq 0, \\ \frac{1}{\|a_k\| \cdot \|a_l\|} \sum_{i=0}^{N+m-1} a_{k,i} a_{l,i-m}^*, & m < 0, \end{cases} \qquad (7)$$

где в (6) $\rho(m)$ - апериодическая АКФ кодовой последовательности, $\{a_0,a_1,\ldots,a_{N-1}\}$, характеризующая схожесть последовательности со своей копией сдвинутой на m позиций, в (7) $\rho_{a,kl}(m)$ – апериодическая ВКФ кодовых последовательностей $\{a_{k,0},a_{k,1},\ldots,a_{k,N-1}\}$ и $\{a_{l,0},a_{l,1},\ldots,a_{l,N-1}\}$ двух сигналов, характеризующая степень сходства первой последовательности со сдвинутой на m позиций репликой второй [5].

Другим, не менее важным показателем псевдослучайности, полученных последовательностей, применяемым многими авторами, являются тесты FIPS 140-2 предложенные Американским Национальным Институтом Стандартов и Технологий описанные в [6].

Тесты FIPS 140-2 используют следующие проверки:

1. Monobit Test состоит в подсчете количества нулей и единиц в последовательности фиксированной длинны N и считается пройденным в случае попадания количества как нулей, так и единиц в требуемый интервал, приведенный в таблице № 1.
2. Poker Test заключается в проверке независимости и равномерности распределения, состоит в объединении последовательно стоящих 4-х битных последовательностей и подсчете по формуле:

$$N = \frac{16}{5000} \sum_{i=1}^{16} f(i)^2 - 5000 \qquad (8)$$

Далее проверяется попадание значения в требуемый интервал в таблице № 1.

3. Run Test состоит в подсчете количества последовательностей рядом стоящих последовательностей ‘010’ и ‘101’ для Run Test – 1, тест считается пройденным при попадании в интервал приведенный в таблице № 1. Аналогичные требования существуют и для других размерностей типовых последовательностей.
4. Long Run Test состоит в подсчете последовательностей количества 26-последовательно стоящих единиц и нулей. Тест считается пройденным при отсутствии последовательностей.

Таблица № 1

Требования к тестам FIPS 140-2

Тест	Требуемый интервал для 20000 бит
Monobit Test	9.725 ~ 10.275
Poker Test	2.16 ~ 46.17
Run Test - 1	2493.6 ~ 2506.9
Run Test - 2	1244.9 ~ 1253.8
Run Test - 3	527 ~ 723
Run Test - 4	240 ~ 384
Run Test - 5	103 ~ 209
Run Test – 6+	103 ~ 209

III. РЕЗУЛЬТАТЫ ОЦЕНОК ХАРАКТЕРИСТИК

На рис. 1 приведены временные реализации X,Y,Z модифицированной динамической системы и фазовый портрет.

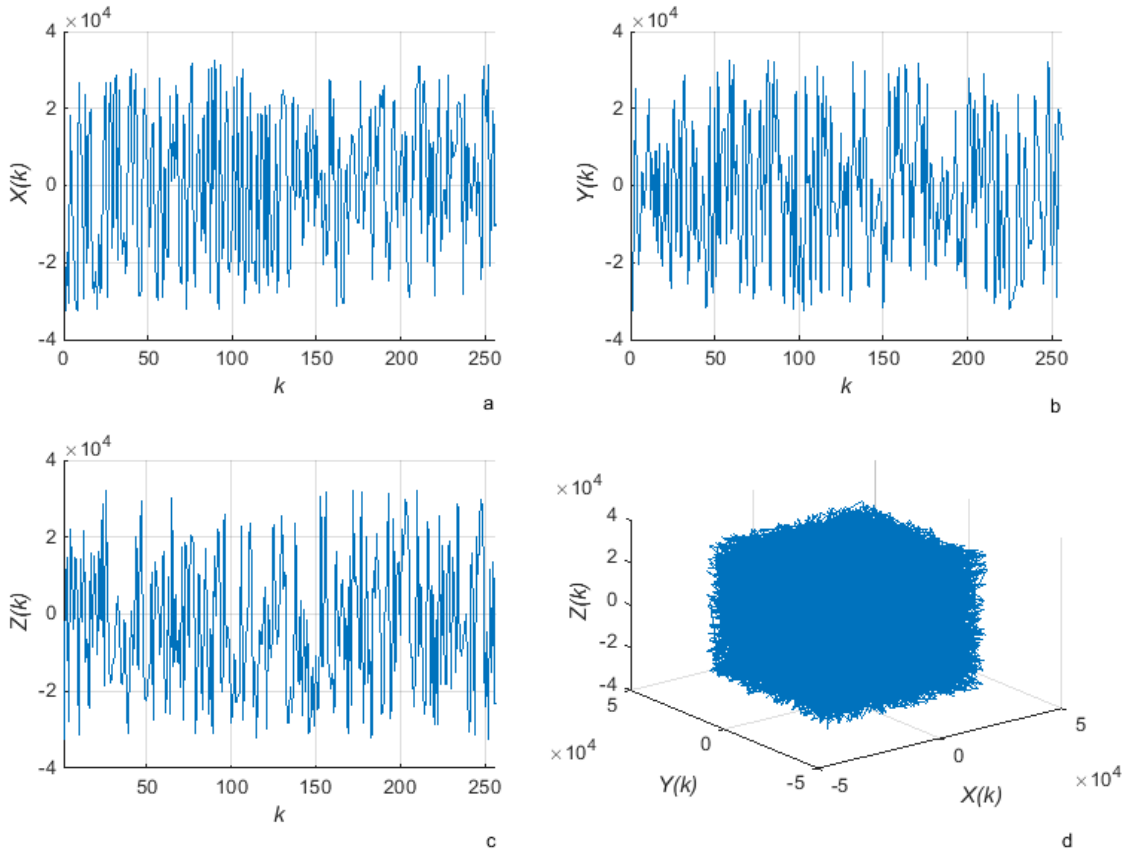

Рис.1. Временная реализация псевдослучайного сигнала построенного на базе системы Лоренца (a, b, c) и фазовый портрет (d)

На рис.1 a, b, c представлены графики временной реализации трех компонент сигнала модифицированной динамической системы. Из рис.1 d видно, что фазовый портрет системы достаточно равномерно заполнен фазовыми траекториями, что подтверждает вывод о сложности режима системы построенной над полем Галуа. Необходимо отметить, что полученные режимы работы системы, как и следовало ожидать, имеют мало общего с исходными динамическими системами. Аналогичные портреты были получены и для систем (2) и (4).

Для оценки равновероятности появления на выходе генераторов 16 битных чисел в работе оценены гистограммы для всех компонент хаотических сигналов систем (1), (2), (4). На рис.2 приведена гистограмма одной из компонент реализации хаотического сигнала системы (1).

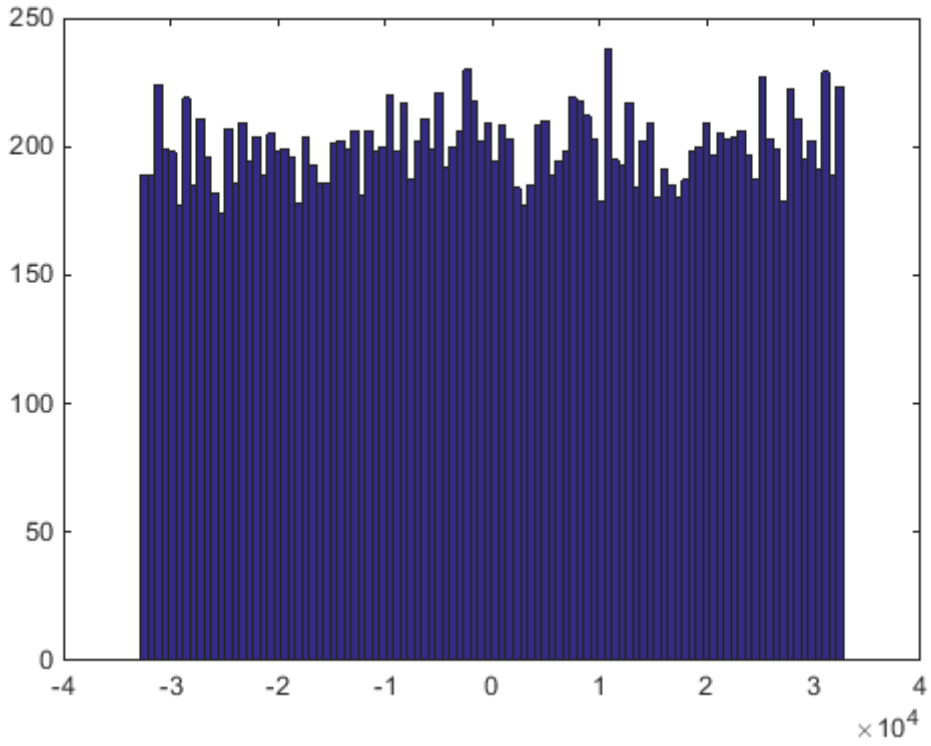

Рис.2. Гистограмма распределения сигнала X системы Лоренца.

При анализе распределений компонент реализации хаотического сигнала была проведена оценка равномерности распределения по критерию χ^2 (5). В соответствии с наложенными ограничениями получившиеся гистограммы сигналов систем (1), (2) и (4) соответствуют равновероятному закону появления 16-битных чисел с доверительной вероятностью не менее 0,95.

В работе выполнен анализ апериодических АКФ и ВКФ кодовых двоичных последовательностей, результаты которого представлены в таблице № 2. Получены оценки максимального и среднего значений боковых лепестков АКФ и ВКФ.

Таблица № 2

АКФ и ВКФ двоичных последовательностей

	АКФ			ВКФ		
Вид системы	Лоренца	Чуа	Дмитриева-Кислова	Лоренца	Чуа	Дмитриева-Кислова
X $R_{max}\sqrt{N}$	5,5906	4,7730	4,4194	4,77	5,01	4,92
Y $R_{max}\sqrt{N}$	4,6404	5,4138	4,4194	4,59	4,77	4,8
Z $R_{max}\sqrt{N}$	4,5520	4,9718	4,9497	4,83	4,55	4,7
X $m_{|R|}\sqrt{N}$	0,5910	0,5792	0,5798	0,556	0,556	0,552
Y $m_{|R|}\sqrt{N}$	0,5795	0,5861	0,5743	0,556	0,556	0,552
Z $m_{|R|}\sqrt{N}$	0,5870	0,5773	0,5786	0,556	0,556	0,556

Для систем Лоренца, Чуа и Дмитриева-Кислова максимальный уровень бокового лепестка составляет не более 0,043 при длине реализации 20000 отсчетов. Из полученных результатов (на основании 2000 опытов) приведенных в таблице № 2 уровней боковых лепестков АКФ и ВКФ, сформированные двоичные сигналы по классификации, Л.Е. Варакина [7] соответствуют «случайным последовательностям».

Сигналы X, Y, Z систем (1), (2), (4) были проверены на соответствие тестам FIPS-140-2:

Для системы Лоренца (1) получены реализации сигналов длиной 20000 бит при вариации параметров r, σ, b. Для каждого из значений параметров было получено 1000 трехмерных реализаций последовательностей, которые подвергались тестированию в соответствии с методикой, приведенной в разделе III. Оценено соответствие реализаций требованиям, приведенным в таблице № 1. Если одна из переменных трехмерных реализаций не проходила хотя бы один из тестов, то тест считался не пройденным. При случайной вариации параметра r системы Лоренца с доверительной вероятностью 0,95 число последовательностей,

удовлетворяющих требованиям теста FIPS 140-2 не менее 991 из 1000. При вариации σ и b число последовательностей не менее 993 из 1000.

Для системы Чуа (2) проведены тесты FIPS-140-2 при изменяющейся нелинейной характеристике системы (параметре N). Система удовлетворяет тестам FIPS-140-2, при этом нижняя граница доверительного интервала вероятности выполнения теста составила 0,9942 при доверительной вероятности 0,95.

Для системы Дмитриева-Кислова (4) были проведены тесты FIPS-140-2 при изменении параметров Q и M. Система удовлетворяет тестам FIPS-140-2, при этом нижняя граница доверительного интервала вероятности выполнения теста составила 0,9952 при доверительной вероятности 0,95.

Таким образом, сформированные двоичные последовательности сигналов удовлетворяют требованиям тестов FIPS 140-2.

IV. ВЫВОДЫ

Синтезирован новый класс генераторов псевдослучайных сигналов на основе модифицированных систем Лоренца, Чуа и Дмитриева-Кислова, реализованных над полем Галуа.

Проведенный анализ временных реализаций сигналов показал, что модифицированные системы Лоренца, Чуа, Дмитриева-Кислова формируют псевдослучайные сигналы с уровнем боковых лепестков автокорреляционных функций и взаимно-корреляционных функций, сопоставимым со случайными последовательностями. Анализ гистограмм показал равновероятность появления 16-битных чисел на выходе генераторов хаотических последовательностей.

Двоичные последовательности на основе модифицированных систем с нижним значением оценки доверительной вероятности 0,95 соответствуют тестам FIPS 140-2.

Литература

1. V.V. Afanasiev, M.P. Danilayev, S.S. Loginov, Y.E. Polskiy Variable multimode models of complex dynamic systems // Proceedings of SPIE Vol. 9156, Optical Technologies for Telecommunications 2013, 91560H (April 4, 2014); DOI:10.1117/12.2054235.

2. Danilaev, M.P., Afanasiev, V.V., Loginov, S.S., Polsky, Y.E. Diagnostics and stabilization of multimode nonlinear radio physics systems (2017) 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SINKHROINFO 2017, paper № 7997516, DOI: 10.1109/SINKHROINFO.2017.7997516

3. S.S. Loginov, V.V. Afanasiev. Poly-Gaussian models in describing the signals of Lorenz dynamic system. // Systems of Signals Generating and Processing in the Field of on Board Communications, 2018, pp. 1-4. DOI: 10.1109/SOSG.2018.8350616.

4. Карлов Н.В., Кириченко Н.А. Колебания, волны, структуры. М.: Физматлит, 2003. 496 с.

5. Ипатов В. Широкополосные системы и кодовое разделение сигналов. – Москва: Техносфера, 2007. 488 с.

6. Lequan Min,Tianyu Chen, Hongyan Zang Analysis of FIPS140-2 Testand Chaos-Based Pseudorandom Number Generator. // Chaotic Modeling and Simulation (CMSIM) pp. 2:273-280, 2013.

7. Л.Е. Варакин Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с., ил.

8. M.Yu. Zuev, S.S. Loginov Generation of pseudo-random signals based on a modified Lorenz system, realized over a Galois finite field. // Systems of Signals Generating and Processing in the Field of on Board Communications, 2018, pp. 1-4. DOI: 10.1109/SOSG.2018.8350594.

9. Логинов С.С. Генераторы псевдослучайных сигналов на основе системы Лоренца, реализованной над конечным полем Галуа // Нелинейный мир, №5, т. 15, 2017, с. 26-29.

10. Демьяненко А.В., Топалов Ф.С., Ильин И.В. USB радиомодем // Инженерный вестник Дона, 2015, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2015/2789

11. Кучеренко И.А. Применение сверхширокополосных сигналов с линейной частотной модуляцией в запреградной радиолокации // Инженерный вестник Дона, 2016, № 1 URL: ivdon.ru/ru/magazine/archive/n1y2016/3545

References

1. V.V. Afanasiev, M.P. Danilayev, S.S. Loginov, Y.E. Polskiy. Proceedings of SPIE Vol. 9156, Optical Technologies for Telecommunications 2013, 91560H (April 4, 2014); DOI: 10.1117/12.2054235.

2. Danilaev, M.P., Afanasiev, V.V., Loginov, S.S., Polsky, Y.E. Diagnostics and stabilization of multimode nonlinear radio physics systems (2017) 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SINKHROINFO 2017, paper № 7997516, DOI: 10.1109/SINKHROINFO.2017.7997516

3. S.S. Loginov, V.V. Afanasiev. Systems of Signals Generating and Processing in the Field of on Board Communications, 2018, pp. 1-4. DOI: 10.1109/SOSG.2018.8350616.

4. Karlov N.V., Kirichenko N.A. Kolebanija, volny, struktury [Oscillations, waves, structures]. M.: Fizmatlit, 2003. 496 p.

5. Ipatov V. Shirokopolosnye sistemy i kodovoe razdelenie signalov [Broadband Systems and Code Separation of Signals]. Moskva: Tehnosfera, 2007. 488 p.

6. Lequan Min,Tianyu Chen, Hongyan Zang Analysis of FIPS140-2 Testand Chaos-Based Pseudorandom Number Generator. Chaotic Modeling and Simulation (CMSIM) pp. 2:273-280, 2013.

7. L.E. Varakin Sistemy svjazi s shumopodobnymi signalami [Communication systems with noise-like signals]. M.: Radio i svjaz', 1985. 384 p., il.

8. M.Yu. Zuev, S.S. Loginov Systems of Signals Generating and Processing in the Field of on Board Communications, 2018, pp. 1-4. DOI: 10.1109/SOSG.2018.8350594.

9. Loginov S.S. Nelinejnyj mir, №5, Vol. 15, 2017, pp. 26-29.

10. Demyanenko A.V., Topalov F.S., Ilin I.V. Inženernyj vestnik Dona (Rus), 2015, №1. URL: ivdon.ru/ru/magazine/archive/n1y2015/2789

11. Kucherenko I.A. Inženernyj vestnik Dona (Rus), 2016, №1. URL: ivdon.ru/ru/magazine/archive/n1y2016/3545