МРНТИ 47.47
УДК 517.987; 621.38.049.77

10.51889/2959-5894.2023.82.2.021

А.А. Скабылов[1], Д.М. Жексебай[1], М.К. Ибраимов[1], Е.Д.Налибаев[1]*

[1]Казахский национальный университет имени аль-Фараби, г. Алматы, Казахстан
[*] e-mail: skabylov212@gmail.com

ПРИМЕНЕНИЕ ХАОТИЧЕСКИХ ГЕНЕРАТОРОВ ДЛЯ СЕКРЕТНОГО КЛЮЧА В ПРИЕМО-ПЕРЕДАЮЩИХ ЭЛЕКТРОННЫХ УСТРОЙСТВАХ

Аннотация

Хаотические генераторы псевдослучайных последовательностей (ПСП) на основе программируемых логических интегральных схем (ПЛИС) являются эффективным средством получения высокоэнтропийных ПСП с отличными свойствами статистической независимости. В данной статье рассмотрены основные принципы работы таких генераторов и представлены примеры их реализации на нелинейных динамических системах, включая системы Чуа и Ресслера. Хаотические генераторы обладают сложным детерминированным поведением, которое позволяет получать псевдослучайные последовательности высокой сложности. Использование ПСП на основе хаотических генераторов находит применение в различных областях науки и техники, таких как шифрования данных, радиосвязь и передача информации. Дальнейшее исследование и разработка хаотических генераторов может привести к расширению их применимости в современных технологиях и обеспечить высокий уровень безопасности и эффективности в различных системах.

Ключевые слова: хаотический генератор, динамические системы, FPGA, информационные технологии, цифровые схемы, криптография.

Аңдатпа

Ә.Ә. Сқабылов[1], Д.М. Жексебай[1], М.К. Ибраимов[1], Е.Д.Налибаев[1]
[1]әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы қ., Қазақстан

ЭЛЕКТРОНДЫҚ ҚҰРЫЛҒЫЛЫҚТАРДЫ ҚАБЫЛДАУ ЖӘНЕ ЖЕТКІЗУДЕ ҚҰПИЯ КІЛТ ҮШІН ХАОСТЫҚ ГЕНЕРАТОРЛАРДЫ ҚОЛДАНУ

Программаланатын логикалық интегралдық схемаларға (ПЛИС) негізделген хаостық псевдо кездейсоқ реттілік (ПКР) генераторлары тамаша статистикалық тәуелсіздік қасиеттері бар жоғары энтропиялы ПКР алудың тиімді құралы болып табылады. Бұл мақалада мұндай генераторлардың жұмысының негізгі принциптері қарастырылады және оларды сызықты емес динамикалық жүйелерде, соның ішінде Чуа және Ресслер жүйелеріне енгізу мысалдары келтірілген. Хаостық генераторлар күрделі детерминирленген әрекетке ие, бұл жоғары күрделіліктегі псевдокездейсоқ тізбектерді алуға мүмкіндік береді. Хаостық генераторларға негізделген ПКР пайдалану криптография, радиобайланыс және ақпаратты беру сияқты ғылым мен техниканың әртүрлі салаларында қолдануды табады. Хаостық генераторларды одан әрі зерттеу және дамыту олардың заманауи технологияларда қолдану аясын кеңейтуге әкелуі мүмкін және әртүрлі жүйелерде қауіпсіздік пен тиімділіктің жоғары деңгейін қамтамасыз етеді.

Түйін сөздер: хаостық генератор, динамикалық жүйелер, FPGA, ақпараттық технологиялар, цифрлық схемалар, криптография.

Abstract

APPLICATION OF CHAOTIC GENERATORS FOR A SECRET KEY IN TRANSMIT-RECEIVING ELECTRONIC DEVICES

Sqabylov A.A. [1], Zheksebay D.M. [1], Ibraimov M.K. [1], Nalibaiyev E.D.[1]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan

Chaotic pseudo-random sequence generators (PRS) based on field-programmable gate arrays (FPGAs) are an effective tool for obtaining high-entropy PRSs with excellent statistical independence properties. This article discusses the basic principles of operation of such generators and presents examples of their implementation on nonlinear dynamic systems, including Chua and Ressler systems. Chaotic generators have a complex deterministic behavior that makes it possible to obtain pseudo-random sequences of high complexity. The use of PRS based on chaotic generators finds application in various fields of science and technology, such as data encryption, radio communications, and information transmission. Further research and development of chaotic generators can lead to the expansion of their applicability in modern technologies and provide a high level of safety and efficiency in various systems.

Keywords: chaotic generator, dynamic systems, FPGA, information technology, digital circuits, cryptography.

Введение

В настоящее время, использование псевдослучайных последовательностей (ПСП) является неотъемлемой частью многих информационных технологий и криптографических систем [1]. Эффективное использование ПСП обеспечивает безопасность и конфиденциальность передачи информации в различных сферах жизнедеятельности человека, начиная от банковской сферы [2] и заканчивая радиосвязью и передачей данных в интернете [3]. Генерация псевдослучайных последовательностей является важным компонентом многих криптографических систем и технологий передачи данных.

Однако, с ростом объемов информации и увеличением числа пользователей в интернете возрастают требования к безопасности и конфиденциальности передачи информации. Существуют различные методы генерации ПСП, такие как линейные конгруэнтные методы [4], методы на основе регистров сдвига [5], методы на основе хэш-функций [6], и другие. Каждый метод имеет свои преимущества и недостатки, и выбор конкретного метода зависит от требуемого уровня безопасности и производительности системы.

Одним из способов генерации ПСП является использование хаотических генераторов, которые обладают высокой энтропией и отличными свойствами статистической независимости [7]. Однако, существует проблема их реализации на практике в виде электронных устройств. Использование хаотических генераторов в криптографических системах требует точной настройки параметров и обеспечения устойчивости к внешним воздействиям. В связи с этим, в настоящее время, проводятся исследования и разработки новых методов генерации ПСП с использованием хаотических генераторов, которые обладают повышенной стабильностью и надежностью в реализации на практике.

Целью данной статьи является рассмотрение возможности реализации хаотических генераторов псевдослучайных последовательностей, на основе программируемых логических интегральных схем (ПЛИС), такой подход позволяет создавать компактные и надежные электронные устройства, способные генерировать ПСП с высокой энтропией, а также исследование их эффективности и возможности использования в криптографических системах. Для достижения данной цели, были поставлены следующие задачи:

- Рассмотреть основные принципы работы хаотических генераторов псевдослучайных последовательностей на основе ПЛИС.
- Проанализировать примеры реализации таких генераторов на нелинейных динамических системах, таких как системы Чуа и Ресслер [8].
- Оценить эффективность и свойства, генерируемых ПСП на основе реализованных хаотических генераторов [9].
- Рассмотреть возможность применения полученных результатов в криптографических системах и дать соответствующие рекомендации [10].

В рамках данной работы ожидается получить конкретные результаты по оценке эффективности и свойств генерируемых ПСП на основе реализованных хаотических генераторов псевдослучайных последовательностей на основе ПЛИС. Будут проведены эксперименты для оценки качества генерируемых ПСП, в том числе их статистических свойств, и будут даны рекомендации по использованию этих последовательностей в криптографических системах.

Также важным аспектом реализации хаотических генераторов псевдослучайных последовательностей на основе ПЛИС является выбор оптимальных параметров схемы, которые обеспечивают стабильную работу генератора и высокое качество генерируемых ПСП. Кроме того, важно учитывать влияние окружающей среды и внешних факторов на работу генератора, а также разработать соответствующие методы тестирования и верификации электронных устройств на основе хаотических генераторов. Для повышения степени надежности и безопасности криптографических систем, генерирующих ПСП на основе хаотических генераторов, возможно использование методов аутентификации и контроля целостности данных.

Материалы и методы

Материалы и методы нашего исследования включали в себя выбор объектов исследования - известные динамические системы, описываемые нелинейными дифференциальными уравнениями или отображениями, такие как системы Ресслера и Чуа [11]. На основе анализа литературы мы выбрали системы Ресслера и Чуа, так как они являются классическими примерами систем с хаотическим поведением. Эти системы широко изучались в научных работах, что позволяет сравнивать результаты

нашего исследования с результатами других авторов. Для получения точных и достоверных результатов мы использовали программный пакет MATLAB Simulink, который является мощным инструментом для моделирования и анализа динамических систем. Для каждой из систем, которые мы исследовали, мы создали подробные блок-схемы, описывающие все компоненты и связи между ними, используя уравнения, описывающие эти системы.

После того, как блок-схемы были созданы, мы провели численное моделирование, используя Simulink, чтобы получить временные ряды для каждой переменной. Для этого мы использовали различные методы численного интегрирования, чтобы решить уравнения системы и получить значения переменных на каждом шаге моделирования. Эти временные ряды позволили нам детально изучить поведение системы в различных условиях и выявить характеристики хаоса.

Один из методов, который мы использовали для анализа хаоса в этих системах, был расчет автокорреляционной функции. Автокорреляционная функция является важным инструментом для анализа временных рядов и может помочь определить наличие или отсутствие корреляции между различными значениями сигнала во времени. Это позволяет исследователям выявлять статистические свойства системы и понимать, как система изменяется во времени. Мы вычислили автокорреляционную функцию случайного сигнала по формуле:

$$r_{xx}[k] = \frac{1}{N}\sum_{n=1}^{N} x[n]x[n+k]$$

Формула автокорреляции для дискретного сигнала которая показывает, как коррелированы значения сигнала в разных точках временного ряда (рисунок 1). Этот метод позволил нам оценить степень хаотичности системы.

Для реализации генераторов динамического хаоса для аппаратной части мы использовали ПЛИС семейства "Xilinx Artix 7", а именно плату "Nexys 4 ddr" и ПЛИС "XC7A100T-1CSG324C". Преимуществом использования ПЛИС семейства "Xilinx Artix 7" является их высокая производительность и гибкость. Эти ПЛИС имеют большое количество логических элементов, блоков памяти и высокоскоростных интерфейсов, что позволяет реализовывать сложные вычислительные задачи, в том числе и для создания генераторов динамического хаоса. Мы произвели детальный анализ алгоритмов генерации динамического хаоса и разработали блок-схемы на MATLAB для создания генераторов. Затем, используя Verilog, мы провели конвертацию схем на язык описания аппаратуры, который позволил нам реализовать и оптимизировать логику генераторов на уровне аппаратуры.

Далее, мы прошивали полученный код на ПЛИС, используя инструменты разработки и среды программирования. Этот процесс включал программирование устройств для создания генераторов и создание соответствующих схем соединения для связи между компонентами. В результате мы получили работающие генераторы динамического хаоса

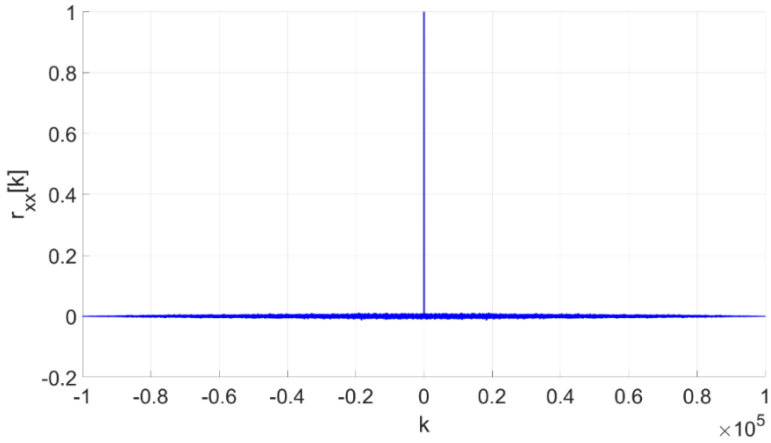

Рисунок 1. Автокорреляционная функция случайного дискретного сигнала

Для численного моделирования системы Росслера мы создали блок-схему (рисунок 2) на MATLAB Simulink, используя уравнения, описывающие эту систему:

$$\dot{x} = -(y + z),$$
$$\dot{y} = x + \alpha y,$$
$$\dot{z} = \beta + z(x - \gamma).$$

При α = 0.2, β = 0.2, γ = 5.7

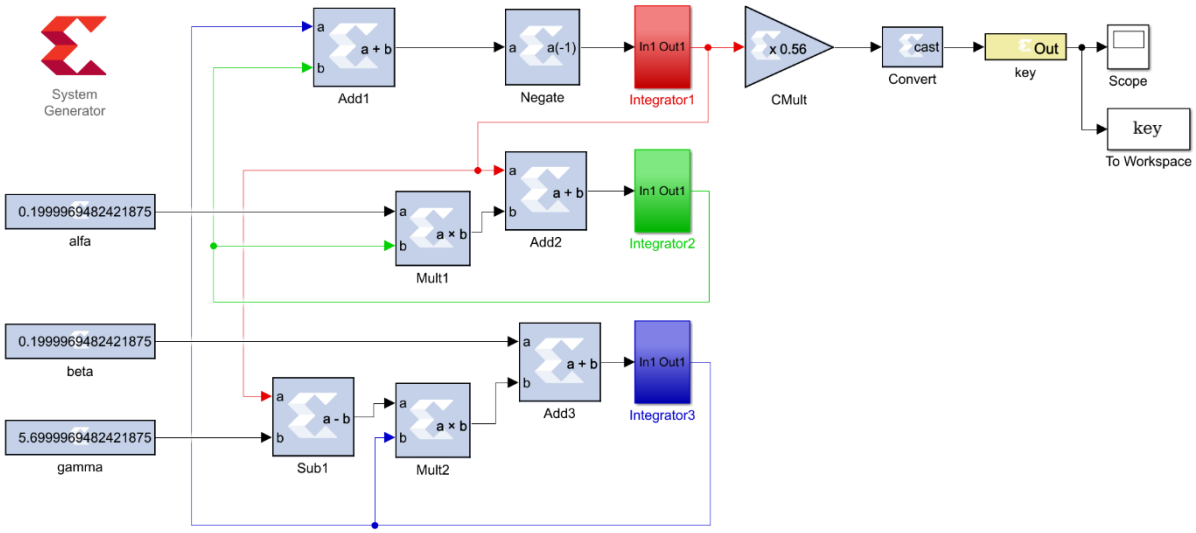

Рисунок 2. Структурная схема системы Росслера

Блок-схема включает в себя три блока, соответствующие переменным состояния x, y и z, а также блоки, соответствующие параметрам α, β и γ.

После создания блок-схемы мы провели численное моделирование системы Росслера, используя Simulink, чтобы получить временные ряды для каждой переменной. Затем мы проанализировали полученные результаты с помощью метода автокорреляционной функции, чтобы определить наличие случайности в системе Росслера (рисунок 3).

Таким образом, блок-схема и численное моделирование системы Росслера в MATLAB Simulink позволили нам исследовать динамику этой системы и определить наличие случайности в ней.

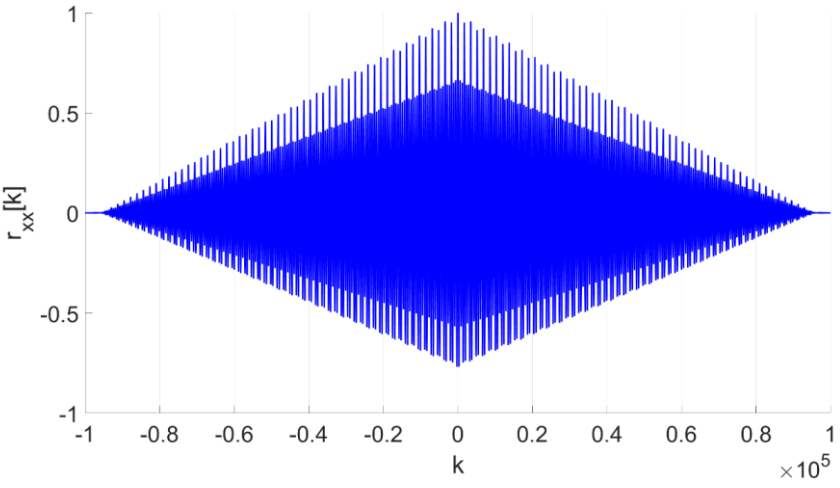

Рисунок 3. Автокорреляционная функция системы Росслера

По результатам моделирования было выявлено, что генератор на основе системы Росслера генерирует числовые значения, которые имеют периодический характер. Это значит, что

последовательность чисел, которые генерируются этой системой, может быть предсказуема и не является случайной.

В связи с этим, использование данной системы для генерации случайных чисел неэффективно, так как не обеспечивает достаточно высокой степени случайности.

Помимо этого, мы также рассмотрели систему Чуа (рисунок 4), которая имеет следующее уравнение:

$$\dot{x} = k\alpha(y - x - g(x)),$$

$$\dot{y} = k(x - y + z),$$

$$\dot{z} = k(-\beta y - \gamma z),$$

$$g(x) = m0x + 0.5(m1 - m0)(|x + 1| - |x - 1|).$$

При: $\alpha = 6.579,\ k = 1, \beta = 10{,}879, m_0 = -0.652, m_1 = -1.812, \gamma = -0.045$

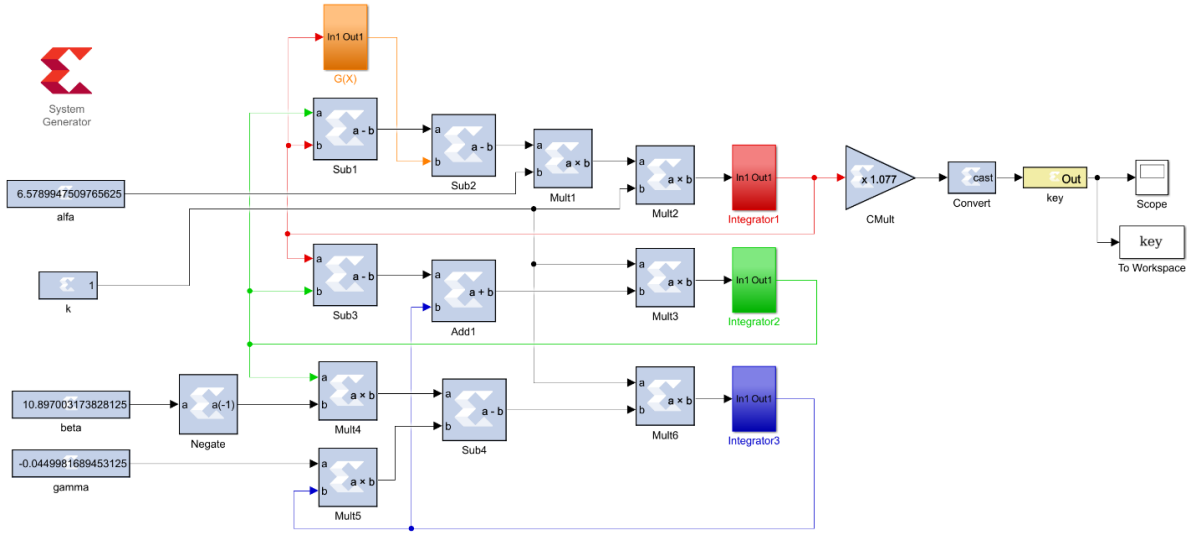

Рисунок 4. Принципиальная схема генератора Чуа

После этого мы построили автокорреляционную функцию для сгенерированных сигналов и проанализировали ее результаты. (рисунок 5).

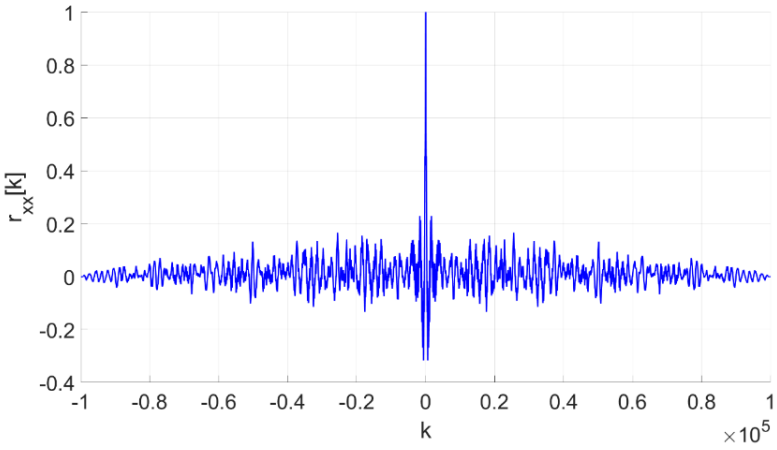

Рисунок 5. Автокорреляционная функция генератора Чуа

Согласно полученным данным, генерация сигнала в системе Чуа близка к случайному сигналу, что делает ее подходящей для генерации случайных чисел. В частности, случайное число, сгенерированное этим генератором, может быть использовано в качестве ключа для шифрования, путем генерации.

Результаты и обсуждение

Ниже представлены результаты реализации системы шифрования на основе генератора Чуа, которые были использованы для создания секретных ключей. На рисунке 6 показана RTL-схема системы (рисунок 6.).

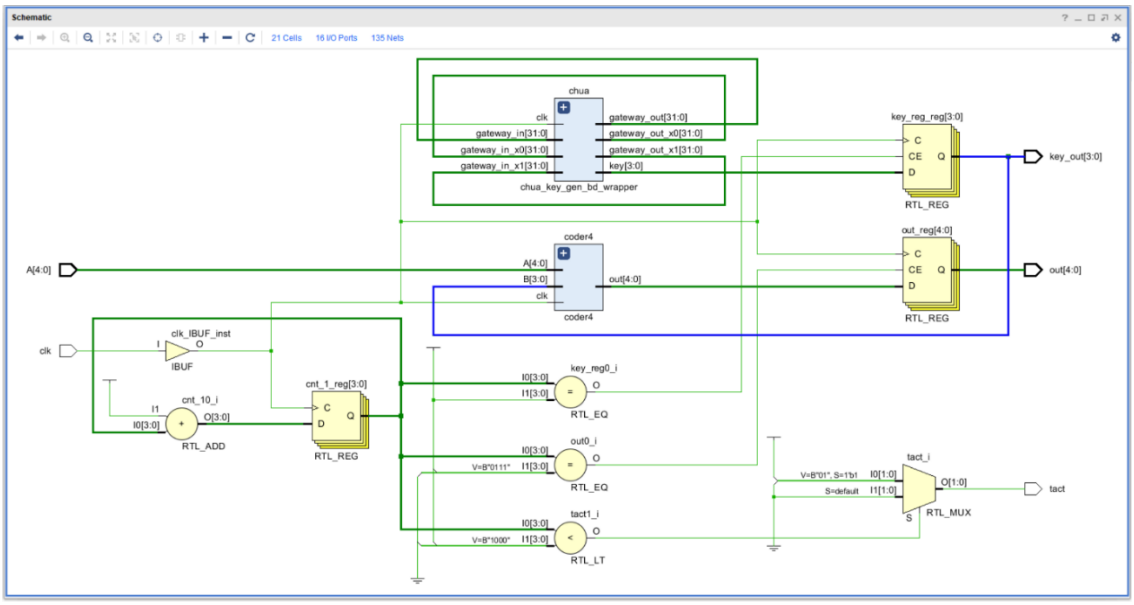

Рисунок 6. Структурная схема блока шифрования (RTL)

RTL-схемы системы Чуа были разработаны для реализации системы на чипе ПЛИС. Они позволяют управлять генерацией случайных чисел и генерировать секретные ключи для использования в качестве ключей шифрования (рисунок 7).

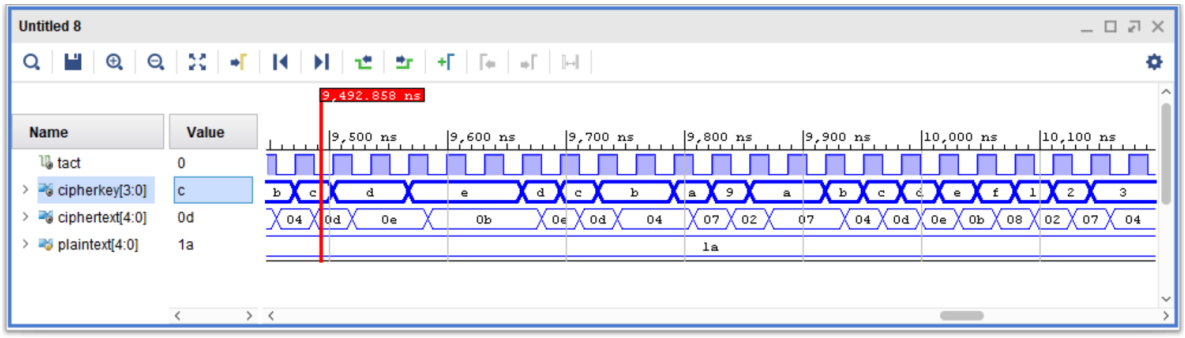

Рисунок 7. Результат проверки алгоритма шифрования

Численное значение тестирования системы Чуа были использованы для отладки и тестирования системы на чипе ПЛИС. Они позволяют контролировать процесс генерации случайных чисел и обнаруживать возможные ошибки и сбои в системе.

В ходе нашего исследования мы провели сравнительный анализ двух систем - Росслера и Чуа. Мы построили автокорреляционные функции для каждой системы и сделали вывод, что генерация сигнала в системе Чуа близка к случайному сигналу, что делает ее подходящей для генерации случайных чисел. Мы также рассмотрели применение системы Чуа для создания ключей шифрования и реализовали алгоритм шифрования на основе ПЛИС.

Обсуждение

1) Эффективность генерации случайных чисел: исследование показало, что генератор на основе системы Чуа может генерировать случайные числа, подходящие для использования в качестве секретных ключей при шифровании данных. Это может быть полезно во многих областях, включая криптографию и статистическую моделирование.

2) Сравнение с другими системами: мы провели сравнительный анализ генераторов на основе систем Росслера и Чуа, и показали, что генерация сигнала в системе Чуа близка к случайному сигналу, в то время как система Росслера не является эффективной для генерации случайных чисел. Это может помочь в выборе наиболее подходящей системы для конкретной задачи.

3) Применение системы Чуа: система Чуа может быть использована не только для генерации случайных чисел, но и для решения многих других задач, включая прогнозирование и управление хаотическими системами. Исследование ее применения может быть интересным направлением для дальнейших исследований.

4) Реализация на чипе ПЛИС: мы использовали чип ПЛИС для реализации системы шифрования на основе генератора Чуа. Это может быть полезно для разработки быстрых и безопасных систем шифрования для различных приложений.

5) Ограничения и перспективы: в ходе исследования мы выявили некоторые ограничения генератора на основе системы Чуа, такие как зависимость от начальных условий и возможность влияния внешних факторов на процесс генерации. Дальнейшее исследование может быть направлено на устранение этих ограничений и на разработку новых методов генерации случайных чисел на основе хаотических систем.

Заключение

В результате нашего исследования мы подтвердили, что система Чуа может быть использована для генерации случайных чисел и создания ключей шифрования. Мы провели анализ системы Чуа и получили автокорреляционную функцию, которая показала близость генерируемого сигнала к случайному сигналу. Использование системы Чуа для генерации ключей шифрования может быть эффективным способом защиты конфиденциальной информации. Однако, необходимо учитывать возможные ограничения и уязвимости данной системы, которые могут быть использованы злоумышленниками для расшифровки зашифрованных сообщений.

Дальнейшее развитие этой работы может включать более глубокое исследование других систем, которые могут быть использованы для генерации случайных чисел и создания ключей шифрования. Также возможно улучшение алгоритма шифрования на основе ПЛИС, используя более сложные математические методы и алгоритмы.

Список использованной литературы:

1 O'Connor, L. et al. (2021). Cryptographic Applications of Chaos-Based Pseudorandom Number Generators: A Review. Entropy, 23(1), 1-30. https://doi.org/10.3390/e23010016

2 Brzeski, P. et al. (2018). FPGA-based True Random Number Generator Utilizing Chaotic Circuit. IEEE Transactions on Circuits and Systems I: Regular Papers, 65(11), 3913-3925. https://doi.org/10.1109/TCSI.2018.2855096

3 Li, H. et al. (2019). A New Chaotic Encryption Algorithm Based on Multi-Dimensional Lorenz System. Complexity, 2019, 1-8. https://doi.org/10.1155/2019/8736018

4 Raj S. Katti; Rajesh G. Kavasseri (2008). Secure pseudo-random bit sequence generation using coupled linear congruential generators. 2008 IEEE International Symposium on Circuits and System, 0271-4302, https://doi.org/10.1109/ISCAS.2008.4542071

5 Gaeini, Ahmad; Mirghadri, Abdolrasoul; Jandaghi, Gholamreza; Keshavarzi, Behbod (2016). A New Pseudo-Random Number Generator Based on Chaotic Maps and Linear Feedback Shift Register. Journal of Computational and Theoretical Nanoscience, Volume 13, Number 1, pp. 836-845(10), https://doi.org/10.1166/jctn.2016.4883

6 Hwajeong, S. et al. (2014). Pseudo random number generator and Hash function for embedded microprocessors. 2014 IEEE World Forum on Internet of Things (WF-IoT), 14255643, https://doi.org/10.1109/WF-IoT.2014.6803113

7 Cao, H. et al. (2017). A New Pseudorandom Number Generator Based on Multimodal Chaotic Map. Complexity, 2017, 1-7. https://doi.org/10.1155/2017/5948790

8 Gao, Y. et al. (2022). FPGA Implementation of Chaos-based Stream Cipher with Synchronization between Transmitter and Receiver. IEEE Transactions on Circuits and Systems II: Express Briefs, 69(3), 504-508. https://doi.org/10.1109/TCSII.2021.3100485

9 Yang, H. et al. (2016). A Chaotic Stream Cipher Using the Internal States of a Three-Dimensional Autonomous Chaotic System. IEEE Transactions on Circuits and Systems II: Express Briefs, 63(12), 1149-1153. https://doi.org/10.1109/TCSII.2016.2607320

10 *Li, X. et al. (2015). Cryptanalysis of a New Chaotic Encryption Algorithm. IEEE Transactions on Circuits and Systems II: Express Briefs, 62(9), 826-830. https://doi.org/10.1109/TCSII.2015.2446711*

11 *Е.Т. Кожагулов, М.К. Ибраимов, С.А. Хохлов, Е. Сагидолда, Д.М. Жексебай. (2014). Генераторы динамического хаоса на программируемых логических интегральных схемах. Вестник. Серия Физическая (ВКФ), [S.l.], v. 49, n. 2, p. 3-7, june 2014. ISSN 2663-2276. https://bph.kaznu.kz/index.php/zhuzhu/article/view/765*

References:

1 O'Connor, L. et al. (2021). Cryptographic Applications of Chaos-Based Pseudorandom Number Generators: A Review. Entropy, 23(1), 1-30. https://doi.org/10.3390/e23010016

2 Brzeski, P. et al. (2018). FPGA-based True Random Number Generator Utilizing Chaotic Circuit. IEEE Transactions on Circuits and Systems I: Regular Papers, 65(11), 3913-3925. https://doi.org/10.1109/TCSI.2018.2855096

3 *Li, H. et al. (2019). A New Chaotic Encryption Algorithm Based on Multi-Dimensional Lorenz System. Complexity, 2019, 1-8.* https://doi.org/10.1155/2019/8736018

4 *Raj S. Katti; Rajesh G. Kavasseri (2008). Secure pseudo-random bit sequence generation using coupled linear congruential generators. 2008 IEEE International Symposium on Circuits and System, 0271-4302,* https://doi.org/10.1109/ISCAS.2008.4542071

5 Gaeini, Ahmad; Mirghadri, Abdolrasoul; Jandaghi, Gholamreza; Keshavarzi, Behbod (2016). A New Pseudo-Random Number Generator Based on Chaotic Maps and Linear Feedback Shift Register. Journal of Computational and Theoretical Nanoscience, *Volume 13, Number 1, pp.* 836-845(10), https://doi.org/10.1166/jctn.2016.4883

6 Hwajeong, S. et al. (2014). Pseudo random number generator and Hash function for embedded microprocessors. 2014 IEEE World Forum on Internet of Things (WF-IoT), 14255643, https://doi.org/10.1109/WF-IoT.2014.6803113

7 Cao, H. et al. (2017). A New Pseudorandom Number Generator Based on Multimodal Chaotic Map. Complexity, 2017, 1-7. https://doi.org/10.1155/2017/5948790

8 Gao, Y. et al. (2022). FPGA Implementation of Chaos-based Stream Cipher with Synchronization between Transmitter and Receiver. IEEE Transactions on Circuits and Systems II: Express Briefs, 69(3), 504-508. https://doi.org/10.1109/TCSII.2021.3100485

9 Yang, H. et al. (2016). A Chaotic Stream Cipher Using the Internal States of a Three-Dimensional Autonomous Chaotic System. IEEE Transactions on Circuits and Systems II: Express Briefs, 63(12), 1149-1153. https://doi.org/10.1109/TCSII.2016.2607320

10 Li, X. et al. (2015). Cryptanalysis of a New Chaotic Encryption Algorithm. IEEE Transactions on Circuits and Systems II: Express Briefs, 62(9), 826-830. https://doi.org/10.1109/TCSII.2015.2446711

11 E.T. Kozhagulov, M.K. Ibraimov, S.A. Hohlov, E. Sagidolda, D.M. Zheksebaj. (2014). Generatory dinamicheskogo haosa na programmiruemyh logicheskih integral'nyh shemah [Dynamic chaos generators on programmable logic integrated circuits]. Vestnik. Serija Fizicheskaja (VKF), [S.l.], v. 49, n. 2, p. 3-7, june 2014. ISSN 2663-2276. https://bph.kaznu.kz/index.php/zhuzhu/article/view/765 (In Russian)