Список использованной литературы:

1 Maldacena J. The large N limit of super conformal field theories and supergravity //Adv. Theor. Math. Phys. – 1998. –Vol.38. – P. 231–252.

2 Karch A., Son D.T., and Starinets A.O. Zero sound from holography // Phys. Rev. Lett. – 2009. – Vol.102. – P. 1103-1125. https://doi.org/10.1103/PhysRevLett.102.051602

3 Gubser S. S., Klebanov I. R. and Polyakov A. M. Gauge theory correlators from non-critical string theory // Phys. Lett. B. - 1998. –Vol. 428. –P. 105. [arXiv:hep-th/9802109]

4 Witten E. Anti-de Sitter space and holography // Adv. Theor. Math. Phys. - 1998. – Vol.2. - P. 253 [arXiv:hep-th/9802150]

5 Landau L. D. The theory of a Fermi liquid // JETP Theoretical Physics. - 1956. – Vol. 30. - P. 1058.

6 Landau L. D. Oscillations in a Fermi liquid // JETP Theoretical Physiks. - 1959. – Vol. 32. - P. 59.

7 Lifshitz E. M. and Pitaevskii L. P., Statistical Physics Part 2 // Pergamon Press, Oxford, 1980. ISBN 0-08-0230-73-5

8 Abrikosov A. A., Gor'kov L. P., and Dzyaloshinskii I. E. Methods of Quantum Field Theory in Statistical Physics // Prentice Hall Englewood Cliffs, NJ. -1963. – Vol.17. – P.1-78.

9 Pines D. and Nozi`eres P. The Theory of Quantum Liquids, Benjamin // New York. -1966. ISSN 978-020147747

10 Quevedo H., Sasha A., Zaldivar. A geometrothermodynamic approach to ideal quantum gases and Bose-Einstein condensates // J. General Relativity and Quantum Cosmology. - 2015. – Vol. 1. – P. 1512-1535. arXiv:1512.08755v3

11 Harry L. Morrison, James V. Lindesay, Uwe K. Albertin Quantum theory of the two-dimensional Bose liquid // Physics Letters A. – 1985. –Vol. 8. – P.397-400.

12 Karch A., O'Bannon A. Holographic thermodynamics at finite baryon density: some exact results // JHEP 0711. - 2007. – Vol. 074. – P. 256. https://doi.org/10.1088/1126-6708/2007/11/074

13 Quevedo H., Sanchez A., Taj S., Vazquez A., Phase transitions in Geometrothermodynamics // Gen.Relativistic Gravity. - 2011. - Vol. 43. – P. 1153. https:doi.org/10.1007/s10714-010-0996-2

14 Quevedo H. Geometrothermodynamics // J. Math. Phys. – 2007. – Vol. 48. - P.013506. Pineda V., Quevedo H., Maria N. Quevedo, Sanchez A., Valdes E. The physical significance of geometrothermodynamic metrics // J. of Geometric Methods in Modern Physics. - 2019. – Vol.16. – No. 11. – P.1950168. https:doi.org/10.1142. /S0219887819501688

15 Engelhardt N and Horowitz G.T. Recovering the spacetime metric from a holographic dual // Adv. Theoretical Math. Phys. - 2017. – Vol. 21. No.7. – P.1635-1653.

МРНТИ 29.01.01.
УДК 621.391
DOI: https://doi.org/10.51889/2020-1.1728-7901.36

А. Заурбек[1], Д.З.Джурунтаев[1]

[1]Satpaev University, г. Алматы, Казахстан

СХЕМА ЦИФРОВОГО ГЕНЕРАТОРА С УВЕЛИЧЕННЫМ ПЕРИОДОМ ПОВТОРЕНИЯ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ИМПУЛЬСОВ

Аннотация

В данной работе рассматривается вопрос модернизации схемы цифрового генератора псевдослучайной последовательности импульсов, который может быть использован для создания криптографических алгоритмов шифрования. Необходимость модернизации схемы цифрового генератора связана с увеличением количества формируемых на его выходе последовательности импульсов псевдослучайной длительности и с псевдослучайными интервалами между ними. Для достижения этой цели в схему цифрового генератора псевдослучайной последовательности импульсов, построенного на основе пятиразрядного регистра сдвига с линейной обратной связью, включены небольшое количество дополнительных элементов.

На основе модернизированной схемы цифрового генератора псевдослучайной последовательности импульсов и активного RC фильтра нижних частот второго порядка Саллена-Ки построен цифровой генератор акустического шума, который в отличие от прототипа имеет истинно случайный характер выходного сигнала в пределах периода ~ $4*(2^N - 1)$ при соблюдении схемотехнической простоты.

Ключевые слова: цифровой генератор псевдослучайной последовательности импульсов, регистр сдвига с линейной обратной связи, логический элемент XOR, фильтр нижних частот второго порядка.

Аңдатпа
А. Заурбек[1], Д.З. Джурунтаев[1]
[1]Satpaev University, Алматы қ., Қазақстан

ПСЕВДО-КЕЗДЕЙСОҚ ИМПУЛЬСТЕР ТІЗБЕГІНІҢ ҰЗАРТЫЛҒАН ҚАЙТАЛАНУ ПЕРИОДЫ БАР ЦИФЛЫҚ ГЕНЕРАТОР СҰЛБАСЫ

Бұл жұмыста криптографиялық шифрлау алгоритмдерін құру үщін пайдалануға болатын псевдо(жалған)-кездейсоқ импульстер тізбегінің сандық генераторының сұлбасын жаңарту туралы мәселені қарастырылған. Цифрлық генератор сұлбасын модернизациялау қажеттілігі оның шығысында пайда болған ұзақтылығы кездейсоқ және олардың арасындағы интервалдары жалған-кездейсоқ ипульстер тізбегі санының артуымен байланысты. Осы мақсатқа жету үшін бес разрядты сызықтық кері байланысы бар ығыстыру регистрі негізінде құрылған жалған-кездейсоқ импульстер тізбегінің сандық генераторының сұлбасына аздаған қосымша элементтер қосылған.

Импульстердің жалған-кездейсоқ тізбегінің сандық генераторының жаңартылған сұлбасы және Саллена-Ки атты екінші ретті төменгі жиілікті белсенді RC фильтрінің негізінде, дыбыстық шудың сандық генераторы жасалынған. Оның, прототипке қарағанда айырмашылығы, қайталану периоды ~ 4 * (2N) – 1) - ға тең аралығында шығыс сигналдары шынымен кездейсоқ және сұлба дизайны қарапайым.

Түйін сөздер: реттілігі псевдокездейсоқ импульстердің цифрлық генераторы, сызықтық кері байланысы бар ығыстыру тіркегіш, логикалық элемент XOR, екінші реттегі төменгі жиілікті фильтр.

Abstract

DIGITAL OSCILLATOR CIRCUIT WITH AN EXTENDED REPETITION PERIOD OF A PSEUDO-RANDOM PULSE SEQUENCE

Zaurbek A. [1], Dzhuruntaev D.Z. [1]
[1]Satpaev University, Almaty, Kazakhstan

In this paper, we consider the issue of upgrading the circuit of a digital generator of a pseudo-random pulse sequence, which can be used to create cryptographic encryption algorithms. The need to modernize the digital generator circuit is associated with an increase in the number of pseudorandom pulse train sequences generated at its output and with pseudorandom intervals between them. To achieve this, a small number of additional elements are included in the circuit of a digital pseudorandom sequence of pulses based on a five-digit shift register with linear feedback.

Based on the modernized circuit of a digital generator of a pseudorandom sequence of pulses and an active second-order Slenlen-Key RC low-pass filter, a digital acoustic noise generator is constructed, which, unlike the prototype, has a truly random output signal over a period of ~ 4 * (2N - 1), subject to circuit simplicity.

Keywords: the digital generator of pseudorandom pulse string, shift register from a linear feed-back, logical element of XOR, filter of lower frequencies the second order.

Введение

У цифровых источников шума «цифровой» шум представляет собой временной случайный процесс, близкий по своим свойствам к процессу физических шумов и называющийся поэтому «псевдослучайным процессом». Генерируемая цифровыми генераторами шума цифровая последовательность двоичных символов представляет собой последовательность прямоугольных импульсов псевдослучайной длительности с псевдослучайными интервалами между ними. Период повторения всей последовательности значительно превышает наибольший интервал между отдельными импульсами последовательности.

Псевдослучайная цифровая последовательность максимальной «длины» – М-последовательности [1], имеющая максимальный период повторения, обычно формируется на основе регистра сдвига, охваченного линейной обратной связью (англ. linear feedback shift register, LFSR), в общем случае многопетлевой. При этом в каждой петле (в цепи обратной связи) регистра сдвига, состоящего из последовательно соединенных триггеров, используются двоичные сумматоры по модулю 2 (логические элементы XOR – «исключающее ИЛИ»). Регистр сдвига LFSR с определенным числом разрядов может синтезировать несколько видов псевдослучайных цифровых последовательностей импульсов. Период повторения псевдослучайных последовательностей импульсов, генерируемых регистром сдвига LFSR зависит от выбранных разрядов для обратной связи регистра [1-4]. Комбинируя варианты включения логических элементов XOR в цепь обратной связи, можно получить последовательности импульсов с различными периодом и структурой.

Максимальный период генерируемой последовательности регистра сдвига LFSR разрядности (длины) N определяется как 2^N-1.

Отсюда для достижения приемлемого периода повторения псевдослучайной последовательности импульсов необходимо увеличить число разрядов регистра сдвига N [2, 5,6].

Целью данной работы является модернизация схемы цифрового генератора псевдослучайной последовательности, обеспечивающей возможность расширения области его применения благодаря формированию последовательности импульсов относительно большего периода, чем 2^N-1.

Методы

В работе на основе регистра сдвига LFSR предлагается схема цифрового генератора псевдослучайной последовательности импульсов, которая может быть использована для создания криптографических алгоритмов шифрования [7,8]. Схема цифрового генератора псевдослучайной последовательности, построенная на регистре сдвига LFSR длиной N (N = 5) с линейными обратными связями и основанная на примитивном трехчлене $x^5 + x^3 = 1$, имеет возможность увеличения периода формируемых псевдослучайных последовательностей импульсов, т. е. формирования случайных импульсов внутри периода ~ $4*(2^N – 1)$, при соблюдении схемотехнической простоты и сравнительно небольшого количества дополнительных элементов.

На основе цифрового генератора псевдослучайной последовательности импульсов, т.е. М-последовательности и активного RC фильтра нижних частот второго порядка Саллена-Ки получена схема генератора акустического шума, которая представлена на рис. 1.

В схему регистра сдвига LFSR для увеличения периода генерируемой последовательности импульсов дополнительно введены новые элементы: второй генератор тактовых импульсов $Г_2$, логические элементы $И_1$, $И_2$, $И_3$, второй сумматор по модулю два XOR_2, логические элементы (ЛЭ) ИЛИ-НЕ и НЕ. Введение новых элементов и их связи с остальными элементами схемы позволяют увеличить период повторения псевдослучайной последовательности импульсов до $4*(2^N – 1)$.

Таким образом, цифровой генератор акустического шума состоит из двух генераторов тактовых импульсов $Г_1$ и $Г_2$, 5-разрядного регистра сдвига с линейной обратной связью на D-триггерах, двух сумматоров по модулю два, трех логических элементов 2И, ЛЭ 2ИЛИ-НЕ и НЕ, активного RC фильтра нижних частот (НЧ) второго порядка Саллена-Ки. К выходу фильтра НЧ подключен пьезоэлектрический вибропреобразователь, который создает акустический шум хаотического характера. Асинхронные входы D-триггеров соединены с входами начальной установки регистра сдвига Ra и Sa. Эти входы подключаются к источникам питания, напряжения которых могут быть равны 0 или 5 В. Рассмотрим работу цифрового генератора акустического шума. 5-ти разрядный регистр сдвига с линейной обратной связью на D-триггерах тактируется прямоугольными импульсами, подаваемыми с выхода тактового генератора $Г_1$. С помощью сумматора по модулю два XOR_1, далее через логические элементы $И_3$ и ИЛИ-НЕ на вход регистра сдвига подается последовательный сигнал, представляющий собой сумму по модулю два 3-го и последнего 5-го разрядов регистра сдвига.

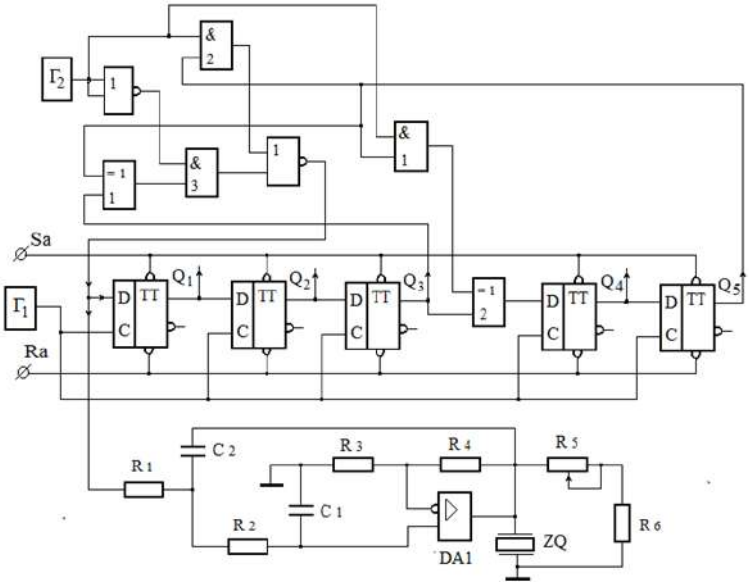

Рисунок 1. Схема цифрового генератора акустического шума

Вначале с помощью сигналов на асинхронных входах Ra (Ra = 5 В) и Sa (Sa = 0 В) регистр сдвига устанавливается в нулевое состояние (можно установить регистр сдвига в единичное состояние с помощью тех же сигналов Ra = 0 В и Sa = 5 В).

После этого на асинхронных входах устанавливаются Ra = 5 В и Sa = 5 В. Для вывода регистра сдвига из нулевого состояния в схему введен ЛЭ ИЛИ-НЕ, формирующий на своем выходе сигнал логической единицы (если начальное состояние регистра сдвига единичное, то на выходе ЛЭ ИЛИ-НЕ будет сигнал логического нуля), который подается на вход D-триггера 1-го разряда.

На выходе регистра сдвига формируются псевдослучайные последовательности импульсов, длительность и интервал между которыми определяются импульсами тактовых генераторов $Г_1$ и $Г_2$, то есть рабочими частотами импульсов этих генераторов. Если примем частоту импульсов тактового генератора $Г_1$, равной 50 кГц, а частоту генератора $Г_2$, равной 5 кГц, тогда регистр сдвига будет поочередно генерировать псевдо-случайные импульсы как регистр сдвига с линейной обратной связью конфигурации Фибоначчи и Галуа [9]. При этом регистр сдвига с линейной обратной связью под воздействием импульсов тактовых генераторов $Г_1$ и $Г_2$ начинает генерировать псевдослучайные импульсы с периодом повторения, равным $\sim 4*(2^N -1)$.

Далее эти импульсы с таким периодом подаются на вход активного RC фильтра нижних частот второго порядка Саллене-Ки и на его выходе формируются акустические шумы хаотического характера. В общем случае цифровой генератор акустического шума может иметь N (в частности, 31) разрядов. При этом количество дополнительных элементов практически не увеличивается, кроме разрядных D-триггеров. Другими словами, с помощью тактового генератора $Г_2$ управляя структурой 5-ти разрядного регистра сдвига при относительно небольшого количества дополнительных элементов (ИЛИ-НЕ, НЕ, трех ЛЭ 2И, и тактового генератора $Г_2$) можно, по сравнению с известными схемами [2,9,12-14], увеличить период повторения импульсов псевдослучайной последовательности примерно в 4 раза. Если N = 31, тогда период повторения $\sim 4*(2^N - 1)$ будет достаточно большим и на выходе цифрового генератора акустический шум хаотического характера практический не будет отличаться от случайного.

Далее для проверки данного технического решения с помощью программы Electronic WorkBench была моделирована схема цифрового генератора шума согласно рис.1.

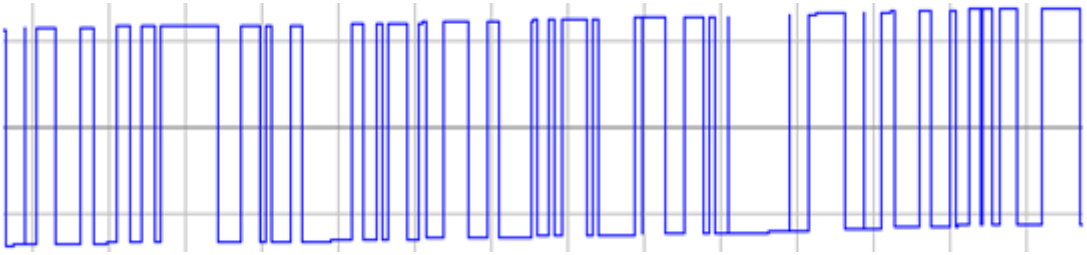

Рисунок 2. Псевдослучайные импульсы цифрового генератора акустического шума

Получены эпюры сигналов в характерных точках цифрового генератора акустического шума, которые представлены на рис.2 и рис.3.

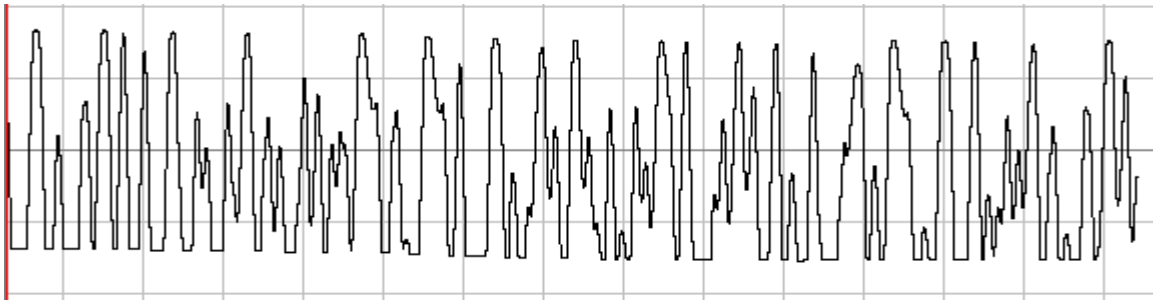

Рисунок 3. Акустические сигналы хаотического характера на выходе цифрового генератора

Эпюрой на рис.2 представлена случайная последовательность импульсов в пределах периода повторения ~ $4*(2^N - 1)$, а эпюра на рис. 3 иллюстрирует хаотически меняющейся акустический сигнал, пропущенный через схему активного фильтра нижних частот второго порядка Саллена-Ки.

В качестве тактовых генераторов $Г_1$ и $Г_2$ можно использовать одну из схем генераторов импульсов на логических элементах, например, схему, приведенную в работе [15].

Результаты

В зависимости от логического состояния импульсов тактового генератора $Г_2$ изменяется структура схемы, вначале, когда импульсы тактового генератора $Г_2$ отсутствуют, т. е. соответствуют логическому нулю схема генерирует псевдослучайные импульсы как цифровой генератор конфигурации Фибоначчи, а когда импульсы тактового генератора $Г_2$ соответствуют логической единице схема генерирует псевдослучайные импульсы как цифровой генератор конфигурации Галуа, а следовательно, на выходе регистра сдвига можно получить хаотические наборы случайных последовательностей в течение времени, равной ~ $4*(2^N - 1)$.

При этом на выходе активного RC фильтра нижних частот второго порядка Саллена-Ки, т. е. на выходе цифрового генератора акустического шума получим хаотический сигнал при относительно небольшого количества дополнительных логических элементов.

Работа относится к области вычислительной техники, информационно-измерительной радиотехники и может быть использовано для защиты речевой информации от несанкционированного доступа путем создания шумового сигнала по акустическим и электронно-оптическим каналам, а также в системах кодирования для генерации псевдослучайных последовательностей.

Список использованной литературы:

1 Брескина О.М., Корешкова А.А., Иванов А.П. Реализация генератора псевдослучайной последовательности на ПЛИС фирмы Altera. – Пенза: Изд-во Пензенского гос. ун-та, 2015. – №5. – С 17-20.

2 Песошин В.А. Генераторы псевдослучайных и случайных чисел на регистрах сдвига.: моногр. / Песошин В.А., Кузнецов В.М. – Казань: Изд-во Казан. гос. техн. ун-та, 2007. – 296 с.

3 Zaurbek A., Seilova N.A, Dzhuruntaev D. Z. Synthesis and simulation of digital pseudo-random impulse sequence generator based on PLIC FPGA Xilinx using CAD Vivado 2016.2 and development of acoustic noise generator scheme for the protection of information. – COMPUTER MODELLING & NEW TECHNOLOGIES 2017 21(1), Scientific and research journal, Mathematical and Computer Modelling, ISSN 1407-5806, ISSN: 1407-5814, Latvia, Riga, 2017. – C.39-46.

4 Zaurbek A., Zhaibergenova A. ZH., Dzhuruntaev D.Z. Developing of the project of a random access memory on FPGA with use of a CAD of QUARTUS II and the Verilog language. – Information Technologies, Management and Society The 16 th International Scientific Conference 2018. April 26-27, ISMA University, Riga, 2018.

5 Ветров Ю.В., Макаров С.Б. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие. – СПб : Изд-во политехн. ун-та, 2011. – 174 с.

6 Патент RU 2446444, G06F7/58, опубл. 27.03.2012.

7 Патент РФ № 2472286, H03B29/00, опубл. 10.01.2013.

8 Заурбек А. Джурунтаев Д.З. Функциональное моделирование регистра сдвига с линейной обратной связью на ПЛИС в среде САПР QUARTUS II с использованием языка VERILOG. – Алматы: Вестник КазНИТУ, 2018. – №6 (130). – С. 97-105.