УДК 004.272.43

А.Н. РЫСОВАНЫЙ, канд. техн. наук, доц. НТУ "ХПИ" (г. Харьков),
В.В. ГОГОТОВ, аспирант НТУ "ХПИ" (г. Харьков)

СРАВНЕНИЕ ДВУХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПО МОДУЛЮ 3 ПО МАКСИМАЛЬНОЙ ДЛИНЕ ФОРМИРУЕМОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Рассмотрена возможность построения генератора псевдослучайных последовательностей (ПСП) по модулю 3 на базе нескольких генераторов псевдослучайных последовательностей по модулю 2. Получена формула, позволяющая рассчитать эффективность генератора ПСП по модулю 3 с использованием блока сложения по модулю 3 по отношению к генератору ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2 по максимальной длине формируемой последовательности. Результаты исследования позволят разработать способ построения генераторов ПСП по большему модулю. Ил.: 2. Библиогр.: 10 назв.

Ключевые слова: генератор псевдослучайных последовательностей, эффективность, блок сложения, длина формируемой последовательности.

Постановка проблемы и анализ литературы. Качество операций генерации случайных последовательностей определяется, в первую очередь, качеством используемых генераторов псевдослучайных последовательностей (ПСП). Именно от свойств генераторов ПСП зависит надежность процесса сбора, обработки, хранения и передачи информации [1].

Для выбора основных характеристик генератора, по которым можно было бы судить о его применимости, необходимо провести анализ генераторов с различной архитектурой построения, рассмотреть влияние архитектуры генератора на максимальную длину формируемой последовательности. В связи с чем необходимы способы исследования характеристик генераторов псевдослучайных последовательностей и сравнения между собой различных генераторов. Также требуются количественные критерии, по которым можно было бы сравнить несколько генераторов ПСП. Таким критерием, например, может быть максимальная длина формируемой последовательности.

В отечественной и зарубежной литературе основное внимание при формировании псевдослучайных чисел уделено генераторам псевдослучайных последовательностей, построенным на основе регистра сдвига с линейной обратной связью (с сумматорами по модулю два), причем в большинстве работ рассматриваются последовательности максимальной длины [2 – 3].

При разработке программных средств генерации ПСП возникает проблема, которая связана с отсутствием инструментальных средств для статического исследования формируемых последовательностей. Более того, этим исследованиям уделялось мало внимание. За последние несколько лет ситуация кардинально изменилась, специалисты признали значимость статистического тестирования. Об этом свидетельствуют многочисленные

факты. В [4 – 8] рассмотрены свойства и особенности последовательностей максимальной длины, показан подход к построению генераторов псевдослучайных последовательностей, получения матриц состояний. Национальный Институт Стандартов и Технологий США (НИСТ) выпустил многостраничное руководство [9] по статическому тестированию генераторов ПСП. Однако [10] "значительная часть установленных здесь фактов – не доказанные теоремы, а эмпирические наблюдения, ожидающие смелых исследователей".

Существует утверждение о том, что генератор псевдослучайных последовательностей по модулю 3 возможно построить на базе нескольких генераторов псевдослучайных последовательностей по модулю 2 с сохранением всех свойств и характеристик, которые будут соответствовать генератору ПСП по модулю 3 с использованием блока сложения по модулю 3. Данное утверждение можно подтвердить или опровергнуть, проведя исследование формируемых генераторами ПСП, а также сравнить максимальную длину формируемой генераторами последовательности в обоих случаях.

Целью статьи является сравнение двух генераторов псевдослучайных последовательностей по максимальной длине формируемой последовательности: генератора по модулю 3 с использованием блока сложения по модулю 3 и генератора по модулю 3, который построен с использованием двух генераторов по модулю 2.

Основная часть. Для построения нелинейного генератора ПСП с использованием блока сложения по модулю 3 в схеме вместо традиционного блока сложения по модулю 2 используется блок сложения по модулю 3.

Математическая запись полиномов для регистров сдвига имеет вид: $P(x) = a_0x^n \oplus_k a_1x^{n-1} \oplus_k \ldots \oplus_k a_n$, где при $k = 2$ выполняется сложение по *mod* 2. Если коэффициент при нулевой степени аргумента $a_n = 1$, то такой полином называется характеристическим. Для нелинейных регистров сдвига с обратными связями для конечного поля Галуа $GF(3)$ $a_n = a_0 \in \{1, 2\}$, $a_i \in \{0, 1, 2\}$ при $(i \neq n, 0)$. Таким образом, нелинейные регистры сдвига с обратными связями могут и не быть характеристическими.

Функциональная схема генератора ПСП с использованием блока сложения по модулю 3 с полиномом $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ приведена на рис. 1. Методика построения генераторов ПСП с использованием блока сложения по модулю 3 описана в [4 – 8].

Число состояний l для такого генератора будет определяться выражением:

$$l = p^m - 1 \qquad (1)$$

Таким образом, для генератора ПСП с использованием блока сложения по модулю 3 с полиномом $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$ максимальная длина формируемой последовательности равна $l = 3^4 - 1 = 80$.

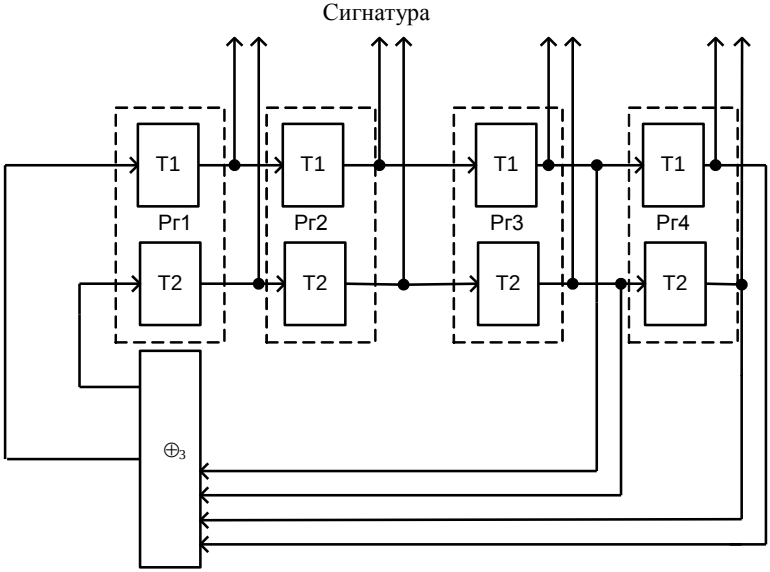

Рис. 1. Функциональная схема генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3 с $P(x) = x^4 \oplus_3 x^3 \oplus_3 1$

Работа генератора ПСП с использованием блока сложения по модулю 3 описывается с помощью матрицы состояний, которая для схемы рис. 1 имеет следующий вид:

$$h = \begin{pmatrix} 100110121100210201221010111222011212000200220212200120102112020222211102212100 \\ 010011012110021020122101011112220112120002002202122001201021120202222111022121000 \\ 001001101211002102012210101111222011212000200220212200120102112020222211102212100 \\ 000100110121100210201221010111222011212000200220212200120102112020222211102212210 \end{pmatrix}$$

Функциональная схема генератора ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2 с полиномом $P(x) = x^4 \oplus_2 x^3 \oplus_2 1$ приведена на рис. 2.

Для получения матрицы состояний, которая будет соответствовать матрице состояний генератора ПСП по модулю 3 с использованием блока сложения по модулю 3, в коммутаторе начальных характеристик

псевдослучайных последовательностей задается начальное состояние триггеров второй очереди с помощью реализации функции сдвига.

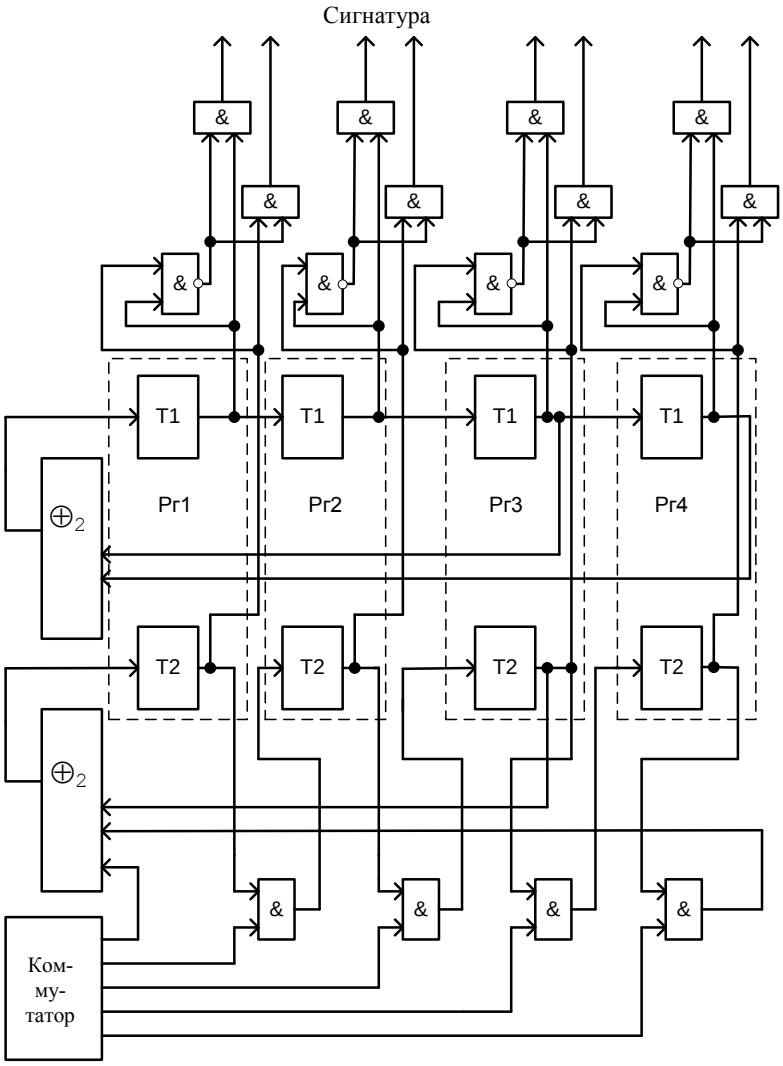

Рис. 2. Функциональная схема генератора псевдослучайных последовательностей по модулю 3, который построен с использованием двух генераторов по модулю 2 с $P(x) = x^4 \oplus_2 x^3 \oplus_2 1$

Снятие данных с соответствующих выходов первой и второй очереди триггеров в результате сформирует новую матрицу состояний, которая будет соответствовать частичной матрице состояний генератора с использованием блока сложения по модулю 3. Формирование элемента новой матрицы будет определяться выражением

$$h_3[i, j] = \left[h_2[i, j],\ h_1\left[shl(h_2[i, j],\ k)\right]\right], \tag{2}$$

где h_3 – новая матрица состояний для генератора ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2; i, j – индексы элемента матрицы; h_2 и h_1 – матрицы состояний генератора ПСП по модулю 2; k – показывает на сколько позиций матрица h_1 сдвинута по отношению к матрице h_2.

Следует отметить, что для h_3 нулевое (0000…), единичное (1111…) и двоичное (2222…) состояние будет являться запрещенным, поскольку на выходах первой или второй очереди триггеров по модулю 2 не сможет сформироваться нулевое состояние.

Число состояний l для такого генератора будет определяться выражением:

$$l = p^m - 3. \tag{3}$$

Таким образом, для генератора ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2 с полиномом $P(x) = x^4 \oplus_2 x^3 \oplus_2 1$ максимальная длина формируемой последовательности равна $l = 3^4 - 3 = 78$.

Принимая во внимание (1) и (2), получим формулу для расчета эффективности генератора ПСП по модулю 3 с использованием блока сложения по модулю 3 по отношению к генератору ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2 по максимальной длине формируемой последовательности:

$$S = \frac{p^m - 1}{p^m - 3}. \tag{4}$$

Работа генератора ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2, описывается с помощью матриц состояний, которые для схемы рис. 2 имеют следующий вид:

$$h_3^{k=1} = \begin{pmatrix} 102012120001002 \\ 210201212000100 \\ 021020121200010 \\ 002102012120001 \end{pmatrix}; \quad h_3^{k=2} = \begin{pmatrix} 122100020011020 \\ 012210002001102 \\ 201221000200110 \\ 020122100020011 \end{pmatrix}; \quad h_3^{k=3} = \begin{pmatrix} 020012020111200 \\ 002001202011120 \\ 000200120201112 \\ 200020012020111 \end{pmatrix};$$

$$h_3^{k=4}=\begin{pmatrix}002102021110001\\200210202111000\\020021020211100\\002002102021110\end{pmatrix};\quad h_3^{k=5}=\begin{pmatrix}120002001101022\\212000200110102\\221200020011010\\022120002001101\end{pmatrix};\quad h_3^{k=6}=\begin{pmatrix}0020021010112 20\\000200210101122\\200020021010112\\220002002101011\end{pmatrix};$$

$$h_3^{k=7}=\begin{pmatrix}122000100110202\\212200010011010\\021220001001101\\202122000100110\end{pmatrix};\quad h_3^{k=8}=\begin{pmatrix}022010121100020\\002201012110001\\200220101211000\\020022010121100\end{pmatrix};\quad h_3^{k=9}=\begin{pmatrix}022110001001202\\202211000100120\\020221100010012\\202022110001001\end{pmatrix};$$

$$h_3^{k=10}=\begin{pmatrix}020112100010022\\202011210001002\\220201121000100\\022020112100010\end{pmatrix};\quad h_3^{k=11}=\begin{pmatrix}000100120101222\\200010012010122\\220001001201012\\222000100120101\end{pmatrix};\quad h_3^{k=12}=\begin{pmatrix}100010021010222\\210001002101022\\221000100210102\\222100010021010\end{pmatrix};$$

$$h_3^{k=13}=\begin{pmatrix}102112000100220\\010211200010022\\201021120001002\\220102112000100\end{pmatrix};\quad h_3^{k=14}=\begin{pmatrix}120102121000200\\012010212100020\\001201021210002\\200120102121000\end{pmatrix}.$$

Выводы. Получен генератор псевдослучайных последовательностей по модулю 3 на базе двух генераторов псевдослучайных последовательностей по модулю 2. В результате исследования было установлено, что максимальная длина формируемой последовательности для такого генератора всегда будет на две последовательности меньше по сравнению с генератором ПСП по модулю 3 с использованием блока сложения по модулю 3. Полученная формула (4) позволяет рассчитать эффективность генератора ПСП по модулю 3 с использованием блока сложения по модулю 3 по отношению к генератору ПСП по модулю 3, который построен с использованием двух генераторов по модулю 2 по максимальной длине формируемой последовательности. Результаты исследования позволят разработать способ построения генераторов псевдослучайных последовательностей по большему модулю.

Список литературы: 1. *Иванов М.А.* Теория, применение и оценка генераторов псевдослучайных последовательностей / *М.А. Иванов, И.В. Чугунков.* – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с. **2.** *Зензин О.С.* Стандарт криптографической защиты XXI века – AES. Теория конечных полей / *О.С. Зензин, М.А. Иванов. Под ред. М.А. Иванова*. – М.: КУДИЦ-ОБРАЗ, 2002. **3.** *Питерсон У.* Коды, исправляющие ошибки / *У. Питерсон, Э. Уэлдон.* – М.: Мир, 1976. **4.** *Рысованый А.Н.* Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины / *А.Н. Рысованый, В.В. Гоготов* // Системи управління, навігації та зв'язку. – К.: Центральний науково-дослідний інститут навігації і управління. – 2007. – Вип.1. – С. 77 – 79. **5.** *Рысованый А.Н.* Методика построения нелинейного генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3 / *А.Н. Рысованый, В.В. Гоготов* // Інформаційно-керуючи системи на залізничному транспорті. – 2008. – Вип. № 5-6. – С. 21 – 25. **6.** *Рысованый А.Н.* Выбор полиномов с *DEGP*(*x*) = 5

для сигнатурных анализаторов в поле Галуа *GF*(3) по критерию формирования последовательности максимальной длинным / *А.Н. Рысованый, В.В. Гоготов* // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: Харківський університет Повітряних Сил імені Івана Кожедуба, 2007. – Вип. 2 (14). – С. 126 – 128. **7.** *Рысованый А.Н.* Выбор полиномов для сигнатурных анализаторов в поле Галуа *GF*(3) по критерию сложности технической реализации / *А.Н. Рысованый, В.В. Гоготов* // Вісник Національного технічного університету "Харківський політехнічний інститут". Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2007. – № 19. – С. 172 – 176. **8.** *Гоготов В.В.* Определение периодической структуры последовательности, порождаемой многочленом с минимальным элементом разложения / *В.В. Гоготов.* // Вісник Національного технічного університету "Харківський політехнічний інститут". Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2009. – № 13. – С. 33 – 38. **9.** A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publications 800-22, 2001. **10.** *Арнольд В.И.* Динамика и статика полей Галуа. Курс лекций / *В.И. Арнольд.* – М.: Мехмат МГУ. – 2004. http://ftp.mccme.ru/

УДК 004.272.43

Порівняння двох генераторів псевдовипадкових послідовностей по модулю 3 по максимальній довжині формованої послідовності / Рисований О.М., Гоготов В.В. // Вісник НТУ "ХПІ". Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2009. – № 43. – С. 172 – 178.

Розглянута можливість побудови генератора псевдовипадкових послідовностей (ПВП) по модулю 3 на базі декількох генераторів псевдовипадкових послідовностей по модулю 2. Отримана формула, що дозволяє розрахувати ефективність генератора ПВП по модулю 3 з використанням блоку складання по модулю 3 по відношенню до генератора ПВП по модулю 3, який побудований з використанням двох генераторів по модулю 2 по максимальній довжині формованої послідовності. Результати дослідження дозволять розробити спосіб побудови генераторів ПВП по більшому модулю. Іл.: 2. Бібліогр.: 10 назв.

Ключові слова: генератор псевдовипадкових послідовностей, ефективність, блок складання, довжина формованої послідовності.

UDC 004.272.43

The comparison of two generators of pseudorandom sequences on the module 3 on the maximum length of the formed sequence / Risavaniy A.M., Gogotov V.V. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2009. – №. 43. – P. 172 – 178.

The possibility of construction of pseudorandom sequence generator on the module 3 is considered on the base of several generators of (PRS) on the module 2. We got the formula allowing to calculate the efficiency of generator of pseudorandom sequences on the module 3 with the use of block of addition on the module 3 in relation to the generator of pseudorandom sequences on the module 3, which is built with the use of two generators on the module 2 on the maximum length of the formed sequence. The results of the research will allow to develop the method of construction of generators of PRS sequences on the greater module. Figs: 2. Refs: 10 sources.

Key words: a generator of pseudorandom sequences, efficiency, block of addition, the length of the formed sequence.

Поступила в редакцию 18.09.2009