Михаил А. Иванов¹, Ирина Г. Коннова², Евгений А. Саликов³, Мария А. Степанова⁴

^{1,3}Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия

^{1,2}Финансовый университет при Правительстве Российской Федерации
(Финансовый университет),
Ленинградский пр-т, 49, Москва, 125993, Россия

^{1,4}Российский государственный университет (НИУ) им. И.М. Губкина,
Ленинский пр-т, 65, корпус 1, Москва, 119991, Россия

¹e-mail: maivanov@mephi.ru, <https://orcid.org/0000-0002-3204-8055>

²e-mail: igkonnova@fa.ru, <https://orcid.org/0000-0003-1228-6256>

³e-mail: esalikov51@gmail.com, <https://orcid.org/0000-0002-3387-1000>

⁴e-mail: maha2702@list.ru, <https://orcid.org/0000-0003-3880-9537>

ОБФУСКАЦИЯ ЛОГИЧЕСКИХ СХЕМ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА РЕГИСТРАХ СДВИГА С ЛИНЕЙНЫМИ И НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

DOI: <http://dx.doi.org/10.26583/bit.2021.1.06>

Аннотация. Цель работы – продемонстрировать возможность использования технологии Logic Encryption для защиты от реверс-инжиниринга логических схем генераторов псевдослучайных чисел на регистрах с линейными и нелинейными обратными связями. Рассматриваемые методы защиты основаны на использовании дополнительных логических элементов в структуре генератора, чтобы скрыть его оригинальные функциональные возможности. Обфускация логической схемы генератора меняет его конструкцию таким образом, что устройство работает правильно, только в том случае, если сигналы на дополнительных ключевых входах генератора принимают правильные значения. Показано, что даже при небольшой разрядности генераторов можно обеспечить огромное количество вариантов реализации ГПСЧ с различным числом состояний и различными свойствами. Введено понятие генератора $(M + 1)$ -последовательности. Продемонстрирована возможность трансформации генераторов $(M - 1)$ - и $(M - 3)$ -последовательностей в генераторы $(M + 1)$ -последовательностей. Главной проблемой IoT является его уязвимость к кибератакам. Предлагаемые методы позволяют повысить безопасность IoT устройств.

Ключевые слова: обфускация, регистр сдвига с линейной обратной связью, регистр сдвига с нелинейной обратной связью, $(M + 1)$ -последовательность, генератор псевдослучайных чисел.

Для цитирования: ИВАНОВ, Михаил А. и др. ОБФУСКАЦИЯ ЛОГИЧЕСКИХ СХЕМ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ НА РЕГИСТРАХ СДВИГА С ЛИНЕЙНЫМИ И НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 74–83, jan. 2021. ISSN 2074-7136. Доступно на: <<https://bit.mephi.ru/index.php/bit/article/view/1322>>. Дата доступа: 08 feb. 2021. DOI: <http://dx.doi.org/10.26583/bit.2021.1.06>.

Michael A. Ivanov¹, Irina G. Konnova², Evgeniy A. Salikov³, Maria A. Stepanova⁴

^{1,3}National Research Nuclear University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31, Moscow, 115409, Russia

^{1,2}Financial University under the Government of the Russian Federation (Financial University),
Leningradskiy Prospekt, 49, Moscow, 125993, Russia

^{1,4}National University of Oil and Gas “Gubkin University”,
Leninskiy Prospekt, 65, building 1, Moscow, 119991, Russia

¹e-mail: maivanov@mephi.ru, <https://orcid.org/0000-0002-3204-8055>

²e-mail: igkonnova@fa.ru, <https://orcid.org/0000-0003-1228-6256>

³e-mail: esalikov51@gmail.com, <https://orcid.org/0000-0002-3387-1000>

⁴e-mail: maha2702@list.ru, <https://orcid.org/0000-0003-3880-9537>

**Obfuscation of logic schemes of pseudo-random number generators
based on linear and non-linear feedback shift registers**

DOI: <http://dx.doi.org/10.26583/bit.2021.1.06>

Abstract. The paper describes methods of protection against reverse engineering of logic circuits of pseudo-random number generators (PRNG) on linear and non-linear feedback shift registers. These methods are based on the use of additional logic elements in the structure of the generator to hide its original functionality. Obfuscation of the generator logic circuit changes its design such that the device works correctly only if the signals at the additional key inputs of the generator take on the correct values. It is shown that even with a small bit capacity of generators, it is possible to provide a huge number of PRNG implementations with different numbers of states and different properties. The concept of a $(M + 1)$ -sequence generator is introduced. The possibility of transforming $(M - 1)$ - and $(M - 3)$ -sequences generators into $(M + 1)$ -sequences generators is demonstrated. The proposed methods can be used to ensure the security of IoT devices.

Keywords: obfuscation, linear feedback shift register, non-linear feedback shift register, $(M + 1)$ -sequence, pseudo-random number generator.

For citation: IVANOV, Michael A. et al. Obfuscation of logic schemes of pseudo-random number generators based on linear and non-linear feedback shift registers. *IT Security (Russia)*, [S.l.], v. 28, n. 1, p. 74–83, jan. 2021. ISSN 2074-7136. Available at: <<https://bit.mephi.ru/index.php/bit/article/view/1322>>. Date accessed: 08 feb. 2021. DOI: <http://dx.doi.org/10.26583/bit.2021.1.06>.

Введение

В последние годы серьезной угрозой безопасности компьютерных систем стало вредоносное аппаратное обеспечение. Из-за аутсорсинга в процессе изготовления интегральных схем (ИС) появляются проблемы, связанные с внедрением аппаратных закладок, подделками ИС, пиратством и несанкционированным перепроизводством.

Наиболее эффективные возможности по предотвращению вышеперечисленных угроз предоставляют технологии Logic Encryption и Design Obfuscation [1–6], реализация второй из них может быть основана на использовании генераторов псевдослучайных чисел (ГПСЧ) с нестандартной диаграммой переключений, например, генераторов $(M - p + 1)$ -последовательностей и генераторов $(M - 2^n + 1)$ -последовательностей, где p – простое, а n – натуральное [7].

В работе рассматриваются особенности применения технологии Logic Encryption для запутывания логической схемы двоичных ГПСЧ (pseudo-random number generator – PRNG) на регистрах сдвига с линейными и нелинейными обратными связями (соответственно linear feedback shift register – LFSR и nonlinear feedback shift register – NLFSR).

1. Регистры сдвига с линейными и нелинейными обратными связями

ГПСЧ на LFSR и NLFSR уже достаточно давно применяются для решения различных задач защиты информации от случайных и умышленных деструктивных воздействий [8–14]. Можно выделить следующие области их использования:

- самотестирование цифровых устройств на БИС;
- вероятностное тестирование цифровых устройств;
- формирование CRC-кодов;
- построение скремблеров и дескремблеров;
- построение ГПСЧ с нестандартными диаграммами переключений;
- построение потоковых и блочных симметричных криптоалгоритмов.

На рис. 1 приведены примеры наиболее распространенных схем ГПСЧ на LFSR и NLFSR, где рассматривается четырехразрядный случай, т.е. $N = 4$, где N – степень характеристического многочлена.

Рис. 1. Четырехразрядные ГПСЧ: а – генератор M -последовательности;
 б – генератор $(M - 1)$ -последовательности; с – генератор $(M - 3)$ -последовательности;
 д – генератор $(M + 1)$ -последовательности. $M = 2^N - 1$

Fig. 1. 4-bit PRNG: а – M -sequence generator; б – $(M - 1)$ -sequence generator;
 с – $(M - 3)$ -sequence generator; д – $(M + 1)$ -sequence generator. $M = 2^N - 1$

На рис. 1,а приведена схема генератора M -последовательности, построенного по схеме Галуа, соответствующего характеристическому многочлену $\varphi(x) = x^4 + x + 1$, примитивному над полем Галуа $GF(2)$. Диаграмма переключений устройства имеет вид 15-1, иначе говоря, состоит из двух кодовых колец, одно длиной 15 включает в себя все ненулевые состояния генератора, второе длиной 1 включает состояние «все нули», переходящее само в себя. Уравнения работы генератора имеют вид:

$$\begin{aligned} q_1(t+1) &= q_4(t), \\ q_2(t+1) &= q_1(t) \oplus q_4(t), \\ q_3(t+1) &= q_2(t), \\ q_4(t+1) &= q_3(t), \end{aligned}$$

где $\oplus$ – операция сложения по модулю два, $q_i(t)$ и $q_i(t+1)$ – содержимое i -го разряда генератора соответственно в моменты времени t и $(t+1)$, $i = 1, 2, 3, 4$.

На рис. 1,б приведен генератор $(M - 1)$ -последовательности, построенный на основе генератора Галуа, соответствующего характеристическому многочлену $\varphi(x) = (x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$, где $\lambda_1(x) = x^3 + x^2 + 1$ – примитивный над полем $GF(2)$. Диаграмма переключений генератора имеет вид 14-2, при этом при корректной работе устройства свертка по модулю два состояния элементов памяти генератора в

каждом такте меняет свое значение на противоположное. Уравнения работы устройства имеют вид:

$$\begin{aligned} q_1(t+1) &= q_4(t) \oplus 1, \\ q_2(t+1) &= q_1(t) \oplus q_4(t) \oplus 1, \\ q_3(t+1) &= q_2(t) \oplus q_4(t) \oplus 1, \\ q_4(t+1) &= q_3(t). \end{aligned}$$

В общем случае при разрядности генератора, равной N , диаграмма переключений генератора $(M-1)$ -последовательности имеет вид $(2^N - 2) - 2$.

На рис. 1,с приведен генератор $(M-3)$ -последовательности, построенный на основе генератора Галуа, соответствующего характеристическому многочлену $\varphi(x) = (x+1)^2(x^2+x+1) = x^4 + x^3 + x + 1$, где $\lambda_2(x) = x^2 + x + 1$ – примитивный над полем $GF(2)$. Диаграмма переключений генератора имеет вид 12-4, при этом при корректной работе устройства в этом режиме свертка по модулю два состояния элементов памяти генератора в каждом такте также меняет свое значение на противоположное. Уравнения работы устройства имеют вид:

$$\begin{aligned} q_1(t+1) &= q_4(t) \oplus 1, \\ q_2(t+1) &= q_1(t) \oplus q_4(t) \oplus 1, \\ q_3(t+1) &= q_2(t), \\ q_4(t+1) &= q_3(t) \oplus q_4(t) \oplus 1. \end{aligned}$$

В общем случае при разрядности генератора, равной N , диаграмма переключений генератора $(M-3)$ -последовательности имеет вид $(2^N - 4) - 4$.

Термины $(M-1)$ -последовательность и $(M-3)$ -последовательность были введены в [11].

На рис. 1,д приведена каноническая схема генератора $(M+1)$ -последовательности, построенного на основе устройства, показанного на рис. 1,а. Диаграмма переключений генератора состоит из одного кодового кольца длиной 16. Когда устройство оказывается в состоянии 1000, единичный сигнал на выходе элемента ИЛИ-НЕ обеспечивает переключение устройства в ранее запрещенное состояние 0000. Сигнал на выходе элемента ИЛИ-НЕ по-прежнему равен единице, поэтому в следующем такте устройство возвращается обратно в основной цикл, переходя в состояние 0100. Уравнения работы генератора имеют вид:

$$\begin{aligned} q_1(t+1) &= q_4(t), \\ q_2(t+1) &= q_1(t) \oplus q_4(t) \oplus z, \\ q_3(t+1) &= q_2(t), \\ q_4(t+1) &= q_3(t), \end{aligned}$$

где z – сигнал на выходе элемента ИЛИ-НЕ,

$$z = \begin{cases} 1, & \text{если } q_2 q_3 q_4 = 000, \\ 0, & \text{в противном случае.} \end{cases}$$

2. Шифрование логики

Рассмотрим базовую идею технологии Logic Encryption. Шифрование логической схемы цифрового устройства (рис. 2,а) дает возможность использовать дополнительные логические элементы в структуре ИС, чтобы скрыть ее оригинальные функциональные возможности. Иначе говоря, это попытка максимально усложнить понимание логики работы защищаемой схемы для неавторизованных лиц. Шифрование логической схемы (по сути ее обфускация) меняет конструкцию ИС таким образом, что она работает правильно, только в том случае, если сигналы на дополнительных ключевых входах устройства принимают правильные значения. Схема обфускации предполагает использование дополнительной схемы преобразования ключей, реализованной на основе

блока памяти с защитой от НСД. Этот блок памяти устанавливается или активируется на заключительном этапе создания ИС перед ее продажей конечному потребителю.

Рис. 2. Шифрование логической схемы цифрового устройства:

a – общая схема; *b* – реализация идеи для ГПСЧ

Fig. 2. Logic encryption in the digital device design: *a* – a general logic encryption scheme; *b* – the general design scheme for PRNG

3. Шифрование логической схемы ГПСЧ

На рис. 2,*b* приведен пример реализации этой идеи, когда защищаемое от реверс-инжиниринга устройство – это ГПСЧ. На рис. 3 показан простейший пример шифрования схемы четырехразрядного генератора, построенного с использованием конструкции Галуа. В зависимости от значений на ключевых входах k_1k_0 устройство реализует одну из четырех диаграмм переключений, приведенных в табл. 1.

Рис. 3. Простейший пример шифрования логической схемы двоичного четырехразрядного ГПСЧ.

Выходами генератора являются выходы разрядов q_1, q_2, q_3, q_4

Fig. 3. A simple logic encryption design of binary 4-bit PRNG. q_1, q_2, q_3, q_4 – generator outputs

Таблица 1. Зависимость диаграммы переключений устройства
от значения ключа k_1k_0

Режим	Ключ	Диаграмма переключений
0	0 0	Два цикла длиной 15 и 1
1	0 1	Четыре цикла длиной 7, 7, 1 и 1
2	1 0	Один цикл длиной 16
3	1 1	Два цикла длиной 14 и 2

На рис. 4 приведен еще один пример реализации шифрования логической схемы с использованием схемы преобразования ключей, реализованной на основе блока замены – классического криптографического примитива. В зависимости от значений на первичных ключевых входах $K_3K_2K_1K_0$ устройство функционирует в одном из 16-ти возможных режимов, некоторые из которых приведены в табл. 2.

Таблица 2. Зависимость диаграммы переключений устройства
от значения Primary Key

$K_3 K_2 K_1 K_0$	$k_4 k_3 k_2 k_1 k_0$	Диаграмма переключений
0 0 0 0	0 0 0 0 1	Два цикла длиной 15 и 1
0 0 0 1	0 0 1 0 0	Два цикла длиной 15 и 1
0 0 1 0	0 0 0 1 1	Четыре цикла длиной 7, 7, 1 и 1
0 0 1 1	0 0 1 1 0	Четыре цикла длиной 7, 7, 1 и 1
0 1 0 0	1 0 0 0 1	Один цикл длиной 16
0 1 0 1	0 0 1 1 1	Четыре цикла длиной 5, 5, 5 и 1
0 1 1 0	0 1 1 1 0	Два цикла длиной 14 и 2
0 1 1 1	0 1 0 1 1	Два цикла длиной 14 и 2
1 0 0 0	0 1 0 0 1	Два цикла длиной 15 и 1
1 0 0 1	0 1 1 0 0	Два цикла длиной 15 и 1
1 0 1 0	0 1 1 0 1	Два цикла длиной 12 и 4
...		

4. Моделирование зашифрованной схемы ГПСЧ

На рис. 5 приведена более сложная схема зашифрованного четырехразрядного PRNG с девятью ключевыми входами, а значит способная выполнять 2^9 различных функций, среди которых 32 варианта генераторов M -последовательностей, 16 вариантов генераторов $(M - 1)$ -последовательностей, 8 вариантов генераторов $(M - 3)$ -последовательностей. Была разработана программа, которая перебирала двоичные наборы на входах $k_8 k_7 k_6 k_5 k_4 k_3 k_2 k_1 k_0$ и определяла для каждого набора соответствующую периодическую структуру генератора. Моделирование работы устройства позволило выявить более десяти необычных режимов работы схемы, один из которых приведен на рис. 6. Схема интересна тем, что генератор дважды «сбивается с ритма», когда при $z = 1$ нарушается закон изменения значения свертки в каждом такте, который реализуется на остальной части диаграммы переключений. Таким образом, выявлена принципиальная

возможность модификации схемы генератора $(M - 1)$ - последовательности и превращения ее в схему генератора $(M + 1)$ - последовательности.

Рис. 4. Простейший пример шифрования логической схемы двоичного четырехразрядного генератора с использованием схемы преобразования ключа:

a – схема устройства с ключевыми входами;

b – схема преобразования ключа на основе блока замены (S-блока)

Fig. 4. A simple logic encryption design of 4-bit PRNG with key transformation scheme:
 a – 4-bit PRNG with key inputs; b – key transformation scheme based on the use of S-box

Рис. 5. Схема зашифрованного двоичного четырехразрядного ГПСЧ

Fig. 5. Encrypted binary 4-bit PRNG

На рис. 5 приведено устройство, построенное на базе генератора Галуа, соответствующего характеристическому многочлену $\varphi(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + 1$ над полем $GF(2)$. Уравнения работы базового генератора имеют вид:

$$\begin{aligned} q_1(t+1) &= q_4(t) \oplus c_1, \\ q_2(t+1) &= q_1(t) \oplus a_1q_4(t) \oplus c_2, \\ q_3(t+1) &= q_2(t) \oplus a_2q_4(t) \oplus c_3, \\ q_4(t+1) &= q_3(t) \oplus a_3q_4(t) \oplus c_4, \end{aligned}$$

где $a_i \in \{0, 1\}$ – коэффициенты многочлена $\varphi(x)$, $c_i \in \{0, 1\}$ – управляющие входы устройства. В общем случае при произвольной разрядности генератора, равной N , уравнения принимают вид:

$$q_1(t+1) = q_N(t) \oplus c_1,$$

Рис. 6. Логика работы двоичного четырехразрядного генератора
 при $k_8 k_7 k_6 k_5 k_4 k_3 k_2 k_1 k_0 = 0 1 0 0 0 1 1 0 1$:

a – эквивалентная схема устройства; b – диаграмма его переключений

Fig. 6. Generator operation logic at key value $k_8 k_7 k_6 k_5 k_4 k_3 k_2 k_1 k_0 = 0 1 0 0 0 1 1 0 1$:

a – generator equivalent circuit; b – generator state transition graph

Заключение

Рассмотрены методы обфускации логических схем генераторов псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. Показано, что даже при небольшой разрядности генераторов можно обеспечить огромное количество вариантов реализации ГПСЧ с различным числом состояний и различными свойствами. Таким образом, обоснована эффективность технологии Logic Encryption применительно к защите от реверс-инжиниринга логической схемы ГПСЧ на регистрах сдвига с линейными обратными связями. Эффективность обусловлена тем, что с ростом разрядности генераторов возрастает число возможных характеристических многочленов максимального периода. В общем случае это число равно $M_2(N)$, где $\varphi(\cdot)$ – число Эйлера. Соответственно растет число возможных канонических вариантов схем генераторов $(M+1)$ -, M -, $(M-1)$ - и $(M-3)$ -последовательностей. В общем случае при разрядности генератора, равной N , эти числа равны

$$N_M = \frac{2^N \varphi(2^N - 1)}{N}, N_{M-1} = \frac{2^{N-1} \varphi(2^{N-1} - 1)}{N-1}, N_{M-3} = \frac{2^{N-1} \varphi(2^{N-2} - 1)}{N-2}.$$

Таким образом, на практике применение идеи запутывания логической схемы устройства помимо решения вышеперечисленных проблем с вредоносным аппаратным обеспечением, подделками ИС, пиратством и несанкционированным перепроизводством позволяет реализовать механизм скрытых (особо защищенных) функций устройства, например, для защиты технического решения от использования по двойному назначению.

Генераторы рассмотренного класса активно используются для реализации минималистских (light-weight) алгоритмов защиты информации, в том числе криптографических. Области использования таких алгоритмов – RFID-технологии и Интернет вещей.

Дальнейшее развитие идеи запутывания схемы двоичного ГПСЧ может быть связано с увеличением числа генераторов $(M + 1)$ -последовательностей, добавлением режимов генерации последовательностей с предпериодом, а также возможности построения генераторов, функционирующих в поле $GF(2^n)$.

СПИСОК ЛИТЕРАТУРЫ:

1. Chakraborty R.S. and Bhunia S., HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection, in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 28, no. 10. P. 1493–1502, Oct. 2009. DOI: <http://dx.doi.org/10.1109/TCAD.2009.2028166>.
2. Tehranipoor M. and Koushanfar F., A Survey of Hardware Trojan Taxonomy and Detection, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 10–25, Jan.-Feb. 2010. DOI: <http://dx.doi.org/10.1109/MDT.2010.7>.
3. Li L. and Zhou H., Structural transformation for best-possible obfuscation of sequential circuits, 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, TX, 2013. P. 55–60, DOI: <http://dx.doi.org/10.1109/HST.2013.6581566>.
4. Baumgarten A., Tyagi A. and Zambreno J. Preventing IC Piracy Using Reconfigurable Logic Barriers, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 66–75, Jan.-Feb. 2010, DOI: <http://dx.doi.org/10.1109/MDT.2010.24>.
5. Chakraborty, Rajat Subhra: Hardware security through design obfuscation, Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy. Thesis Adviser: Dr. Swarup Bhunia. Department of Electrical Engineering and Computer Science. Case Western Reserve University, May, 2010. URL: https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=case1270133481&disposition=inline (дата обращения: 20.01.2021).
6. Becker G.T., Fyrbiak M., Kison C. (2017) Hardware Obfuscation: Techniques and Open Challenges. In: Bossuet L., Torres L. (eds) Foundations of Hardware IP Protection. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-50380-6_6.
7. Ivanov M.A., Kliuchnikova B.V., Salikov E.A., Starikovskii A.V. (2020) New Class of Non-binary Pseudorandom Number Generators. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_35.
8. Dubrova E.A. Scalable Method for Constructing Galois NLFSRs with Period $2^n - 1$ using Cross-Join Pairs. Cryptology ePrint Archive, Report 2011/632, 2011. URL: <http://eprint.iacr.org/2011/632> (дата обращения: 20.01.2021).
9. Dubrova E.A. Method for Generating Full Cycles by a Composition of NLFSRs. URL: <https://eprint.iacr.org/2012/492.pdf> (дата обращения: 20.01.2021).
10. Dubrova E., Teslenko M. and Tenhunen H. 2008. On analysis and synthesis of (n, k) -non-linear feedback shift registers. In Proceedings of the conference on Design, automation and test in Europe (DATE '08). Association for Computing Machinery, New York, NY, USA. P. 1286–1291. DOI: <https://doi.org/10.1145/1403375.1403686> (дата обращения: 20.01.2021).
11. Песошин В.А., Кузнецов В.М. Генераторы псевдослучайных и случайных чисел на регистрах сдвига. Казань: Изд-во Казанского гос. техн. ун-та, 2007. URL: <https://elibrary.ru/item.asp?id=19590566> (дата обращения: 20.01.2021).
12. Кузнецов В.М., Песошин В.А. Генераторы равновероятностных псевдослучайных последовательностей на регистрах сдвига. Известия высших учебных заведений. Поволжский регион. Технические науки. 2012, № 1. С. 21–28. URL: <https://elibrary.ru/item.asp?id=17893013> (дата обращения: 20.01.2021).
13. Кузнецов В.М., Песошин В.А. Генераторы случайных и псевдослучайных последовательностей на цифровых элементах задержки. Казань: Изд-во Казанского гос. техн. ун-та, 2013. – 336 с. URL: <https://elibrary.ru/item.asp?id=32597446> (дата обращения: 20.01.2021).

14. Pesoshin, V.A., Kuznetsov, V.M. & Shirshova, D.V. Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers. Autom Remote Control 77, 1622–1632 (2016). DOI: <https://doi.org/10.1134/S0005117916090095>.

REFERENCES:

- [1] Chakraborty R.S. and Bhunia S., HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection, in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 28, no. 10. P. 1493–1502, Oct. 2009. DOI: <http://dx.doi.org/10.1109/TCAD.2009.2028166>.
- [2] Tehranipoor M. and Koushanfar F., A Survey of Hardware Trojan Taxonomy and Detection, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 10–25, Jan.-Feb. 2010, DOI: <http://dx.doi.org/10.1109/MDT.2010.7>.
- [3] Li L. and Zhou H., Structural transformation for best-possible obfuscation of sequential circuits, 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Austin, TX, 2013. P. 55–60, DOI: <http://dx.doi.org/10.1109/HST.2013.6581566>.
- [4] Baumgarten A., Tyagi A. and Zambreno J. Preventing IC Piracy Using Reconfigurable Logic Barriers, in IEEE Design & Test of Computers. Vol. 27, no. 1. P. 66–75, Jan.-Feb. 2010. DOI: <http://dx.doi.org/10.1109/MDT.2010.24>.
- [5] Chakraborty, Rajat Subhra: Hardware security through design obfuscation, Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy. Thesis Adviser: Dr. Swarup Bhunia. Department of Electrical Engineering and Computer Science. Case Western Reserve University, May, 2010. URL: https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=case1270133481&disposition=inline (accessed: 20.01.2021).
- [6] Becker G.T., Fyrbiak M., Kison C. (2017) Hardware Obfuscation: Techniques and Open Challenges. In: Bossuet L., Torres L. (eds) Foundations of Hardware IP Protection. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-50380-6_6.
- [7] Ivanov M.A., Kliuchnikova B.V., Salikov E.A., Starikovskii A.V. (2020) New Class of Non-binary Pseudorandom Number Generators. In: Misyurin S., Arakelian V., Avetisyan A. (eds) Advanced Technologies in Robotics and Intelligent Systems. Mechanisms and Machine Science, vol 80. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-33491-8_35.
- [8] Dubrova E.A. Scalable Method for Constructing Galois NLFSRs with Period $2^n - 1$ using Cross-Join Pairs. Cryptology ePrint Archive, Report 2011/632, 2011. URL: <http://eprint.iacr.org/2011/632> (accessed: 20.01.2021).
- [9] Dubrova E.A. Method for Generating Full Cycles by a Composition of NLFSRs. <https://eprint.iacr.org/2012/492.pdf> (accessed: 20.01.2021).
- [10] Dubrova E., Teslenko M. and Tenhunen H. 2008. On analysis and synthesis of (n, k) -non-linear feedback shift registers. In Proceedings of the conference on Design, automation and test in Europe (DATE '08). Association for Computing Machinery, New York, NY, USA. P. 1286–1291. DOI: <https://doi.org/10.1145/1403375.1403686> (accessed: 20.01.2021).
- [11] Pesoshin V.A., Kuznetsov V.M. Generatory psevdosluchajnyh i sluchajnyh chisel na registrah sdviga. Kazan: Izd-vo Kazanskogo gos. tehn. un-ta, 2007. URL: <https://elibrary.ru/item.asp?id=19590566> (accessed: 20.01.2021) (in Russian).
- [12] Kuznetsov V.M., Pesoshin V.A. Generatori ravnoveroyatnostnih psevdosluchajnyh posledovatelnostei na registrah sdviga. Izvestiya visshih uchebnyh zavedenii. Povoljskii region. Tehnicheskie nauki. 2012, no. 1. P. 21–28. URL: <https://elibrary.ru/item.asp?id=17893013> (accessed: 20.01.2021) (in Russian).
- [13] Kuznetsov V.M., Pesoshin V.A. Generatori sluchajnyh i psevdosluchajnyh posledovatelnostei na cifrovih elementah zaderjki. Kazan: Izd-vo Kazanskogo gos. tehn. un-ta, 2013. – 336 s. URL: <https://elibrary.ru/item.asp?id=32597446> (accessed: 20.01.2021) (in Russian).
- [14] Pesoshin, V.A., Kuznetsov, V.M. & Shirshova, D.V. Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers. Autom Remote Control 77, 1622–1632 (2016). DOI: <https://doi.org/10.1134/S0005117916090095>.

*Поступила в редакцию – 25 января 2021 г. Окончательный вариант – 01 февраля 2021 г.
Received – January 25, 2021. The final version – February 01, 2021.*