УДК 004.054

ГЕНЕРАТОРЫ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕ БРЕЙНА НА СДВИГОВЫХ РЕГИСТРАХ С НЕЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ

Дербунович Л. В., Караман Д. Г., Осипенко А. Н.

Национальный технический университет "Харьковский политехнический институт"

Предложены метод и алгоритм нахождения нелинейных булевых функций, обеспечивающих генерацию последовательностей де Брейна в сдвиговых регистрах с нелинейной обратной связью.

Постановка проблемы. В традиционных криптографических системах защиты информации современных компьютерно-интегрированных технологий широко используются генераторы псевдослучайных последовательностей максимальной длины для непрерывной генерации ключа в потоковых шифрах. Для генерации ключа, как правило, используются сдвиговые регистры с линейной обратной связью (СРЛОС). Однако уязвимостью этих генераторов является корреляционная связь между последовательностями СРЛОС и выходными ключевыми последовательностями, что приводит к существенному сокращению числа попыток взлома ключа. В [1, 2] показано, что генерация последовательностей де Брейна на сдвиговых регистрах с нелинейной обратной связью (СРНОС) позволяет повысить степень непредсказуемости ключей в потоковых шифрах. Поэтому разработка процедур нахождения обратных связей СРНОС, которые порождают последовательности из 2^n n-мерных векторов (n-разрядность СР) с минимальными аппаратно-программными затратами на реализацию нелинейных булевых функций, является актуальной научно-технической задачей.

Анализ последних достижений и публикаций. Известно, что генераторы последовательностей де Брейна широко используются для генерации псевдослучайных последовательностей и М-последовательностей в технике связи, в системах диагностирования дискретных устройств, в системах защиты информации и т.д. [1-6]. Нахождение последовательности Де Брейна эквивалентно решению задачи нахождения гамильтонова цикла в графе СР. Различные алгоритмы нахождения этих последовательностей приведены в [7, 8]. Алгоритмы, представленные в этих работах, по своей эффективности оцениваются сложностью программных реализаций в битовых операциях и объемах памяти, необходимых для машинной генерации гамильтоновых циклов. Для реализаций этих вычислений требуется выполнить ~O($n\cdot 2^n$) побитовых операций и память (6n) бит для вычисления значения функции ОС на каждом шаге генерации полной последовательности [8, 9]. В [10] предложен алгоритм генерации последовательностей де Брейна, основанный на использовании специального языка программирования NESL и рекурсивной процедуры формирования последовательности на основе гомоморфного отображения графа состояний поразрядного СР в граф состояний (n-1)-разрядного СР [11]. Как показано в [10], трансляция этого алгоритма с языка NESL на язык Си позволяет генерировать последовательность де Брейна длиной 2^{20} за 5 секунд на Spartstation IPC [10].

Цель статьи. Предложены метод и алгоритм нахождения нелинейных булевых функций ОС, порождающих в СР генерацию последовательностей де Брейна, основанные на свойствах гомоморфизма графов состояний СР, построении автоматных моделей остовных деревьев графа СР и формировании правил переходов состояний автомата, образующих гамильтонов цикл в СР.

Основные материалы исследований. Известно, что в графе $G_{(n+1)}$ $(n+1)$-разрядного СР число различных гамильтоновых циклов равно числу остовных деревьев графа G_n [7]. Остовное дерево графа G_n есть связный ориентированный граф без циклов с числом вершин 2^n и числом дуг (2^n-1). В работе использован подход к определению числа остовных деревьев графа G_n, предложенный в [9], который определяется нижеследующим утверждением.

Утверждение 1 [9]. Пусть G_n — n–вершинный граф без петель и B_0 – его матрица инциденций с одной удаленной строкой. Пусть B_0^T — транспонированная матрица к B_0. Тогда определитель $\left|B_0 \times B_0^T\right|$ равен числу различных остовных деревьев графа G_n.

Это утверждение позволяет определить число остовных деревьев для произвольного сильносвязного графа. Так как граф G_n n–разрядного СР является сильносвязным и правильно ориентированным графом, то для вычисления числа остовных деревьев можно воспользоваться более простой процедурой, основанной на использовании его матрицы смежности [9].

Пусть G_n — граф СР, в котором исключены петли в вершинах z_0 и $z_{(2^n-1)}$. Построим матрицу смежности графа G_n размерности $(2^n \times 2^n)$ следующим образом: пересечение i-й строки и i-го столбца матрицы отмечаем числом k_i – полустепень захода вершины z_i; пересечение i-й строки и j-го столбца $(-k_{ij})$ — числом дуг из вершины z_i в вершину z_j. С ростом n число остовных деревьев растёт с ростом числа его дуг. В теории графов решению проблемы нахождения всех остовных деревьев уделялось значительное внимание, так как выбор “наилучшего” дерева, являлся важным оптимизационным критерием при решении сложных технических задач (в теории управления,

при прокладке дорог, газопроводов, линий электропередач, при вычислении определителей матриц в макроэкономической теории и т.д.) [9, 12]. Без снижения общности изложения результатов работы процедуру генерации последовательностей де Брейна на СРНОС будем рассматривать на примере нахождения гамильтоновых циклов в графе G_4 на основе гомоморфных отображений состояний графов G_4 в G_3 соответствующих сдвиговых регистров.

В качестве примера в таблице 1 представлена матрица смежности G_3 – трехразрядного СР, которая позволяет определить число остовных деревьев путем вычисления минора (2^3-1)-го порядка элемента z_0 матрицы смежности G_3. Вычисление определителя D минора элемента z_0 дает величину $D=16$. Таким образом, существует 16 остовных деревьев в графе G_3 с корнем в вершине z_0.

Таблица 1 – Матрица смежности графа G_3

Вершины	z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7
z_0	1	-1	0	0	0	0	0	0
z_1	0	2	-1	-1	0	0	0	0
z_2	0	0	2	0	-1	-1	0	0
z_3	0	0	0	2	0	0	-1	-1
z_4	-1	-1	0	0	2	0	0	0
z_5	0	0	-1	-1	0	2	0	0
z_6	0	0	0	0	-1	-1	2	0
z_7	0	0	0	0	0	0	-1	1

Один из таких способов состоит в использовании элементарных преобразований деревьев для последовательного построения остовов, начиная с некоторого начального [12]. Однако процедурам, основанным на элементарных преобразованиях деревьев, присущ следующий недостаток: для построения нового дерева необходимо привлекать все найденные ранее деревья, что приводит к значительному возрастанию времени вычисления и объема оперативной памяти.

При построении генераторов последовательностей де Брейна на СРНОС возникает задача нахождения тех остовных деревьев в графе $G_{(n-1)}$, которые порождают гамильтоновы циклы в графе G_n с минимальными аппаратурными затратами на реализацию функций обратной связи СР. Так как гамильтонов цикл графа $G_{(n-1)}$ является остовным деревом этого графа, то множество остовных деревьев графа $G_{(n-1)}$ используется для порождения гамильтоновых циклов в графе G_n и т.д. Итеративно применяя эту процедуру, можно найти ограниченное множество остовных деревьев для $k \le (32 \div 34)$, удовлетворяющих указанным выше свойствам.

Для реализации вычислительного алгоритма предложено рассматривать остовное дерево как граф переходов конечного детерминированного автомата с числом состояний равным числу вершин остовного дерева. Тогда множество остовных деревьев графа G_3 трехразрядного СР, можно представить в табличной форме (таблица 2).

Таблица 2 – Таблица переходов автоматных моделей 16-ти остовных деревьев графа G_3.

z(t)	z(t+1)															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
z_1	z_2	z_2	z_2	z_2	z_2	z_2	z_2	z_2	z_3	z_3	z_3	z_3	z_3	z_3	z_3	z_3
z_2	z_4	z_4	z_4	z_4	z_4	z_5	z_5	z_4	z_5	z_4	z_5	z_4	z_4	z_4	z_4	z_4
z_3	z_6	z_7	z_7	z_7	z_6	z_7	z_6	z_7	z_7	z_6	z_6	z_6	z_6	z_6	z_7	z_7
z_4	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0	z_0
z_5	z_2	z_3	z_2	z_3	z_2	z_3	z_3	z_2	z_3	z_3	z_3	z_3	z_2	z_2	z_2	z_2
z_6	z_5	z_4	z_4	z_4	z_5	z_4	z_4	z_4	z_4	z_4	z_4	z_4	z_5	z_4	z_5	z_4
z_7	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6	z_6

По автоматным моделям остовных деревьев графа $G_{(n-1)}$ можно найти множество гамильтоновых циклов в графе G_n n – разрядного СР по представленной ниже процедуре на примере нахождения гамильтонового цикла графа G_4 по остовному дереву графа G_3.

Для автоматной модели остовного дерева №1 из таблицы 2 для всех восьми состояний построим таблицу переходов путем введения в столбце текущих состояний $z(t)$ состояние z_0 и переход $\delta(z_0, 0) = z_0$ (таблица 3).

Таблица 3 – Таблица переходов

$z(t)$	z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7
$z(t+1)$	z_0	z_2	z_4	z_6	z_0	z_2	z_5	z_6

Остовное дерево №1 (таблица 2) представлено на рис. 1а в форме графа, дуги которого отмечены крестиками и значениями булевой функции обратной связи СР f_{oc}, формирующей функцию переходов автоматной модели остовного дерева.

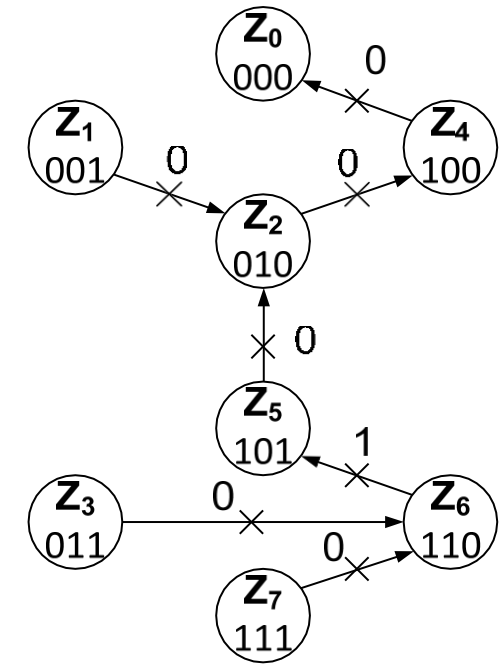
На рис. 1б представлен полный граф G_3 трёхразрядного СР, в котором крестиками отмечены переходы, отображающие переходы состояний остовного дерева с конем в вершине z_0 (рис. 1а). Тогда таблицу переходов полного графа трёхразрядного СР (рис. 1б) можно представить таблицей 4, в которой кружком отмечены переходы, соответствующие переходам автоматной модели остовного дерева (таблица 3).

Свойство гомоморфного отображения графа состояний четырёхразрядного СР графу состояний выбранного остовного дерева №1 трёхразрядного СР, порождающего гамильтонов цикл, обеспечивается следующей процедурой переходов состояний автоматной модели (таблица 4) полного графа G_3 (рис. 1б):

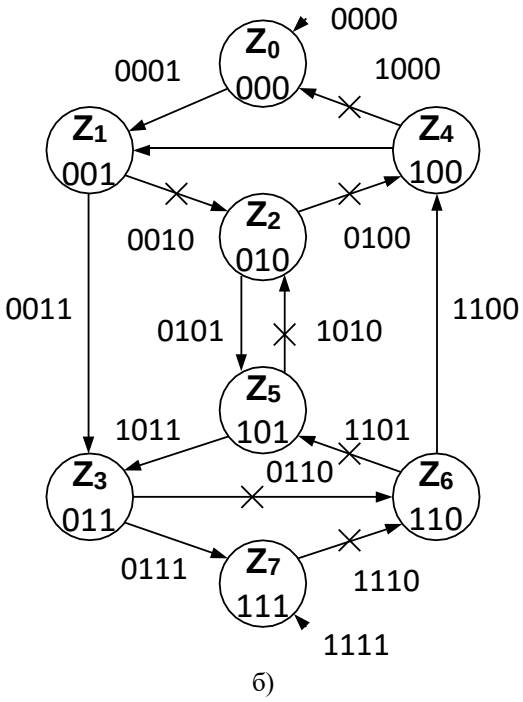
- выбрать начальное состояние z_0;

- для каждого состояния z_i, $i = \overline{0,7}$, выбрать в таблице 4 переход, не отмеченный кружком; если этот

переход использован на предыдущем этапе, то выбрать переход, отмеченный кружком;



а)



б)

Рисунок 1 – Графы переходов G_3 3-разрядного СР а) остовное дерево с корнем в вершине z_0; б) полный граф G_3 с отмеченными дугами

- на каждом шаге определит код состояния z_i^* четырёхразрядного СР по формуле $z_i^* = z_i f_{oc}$ путём добавления (конкатенации) к коду состояния z_i значения $f_{oc} = \{0,1\}$, как это показано на рис. 1б.

- процесс нахождения гамильтонового цикла в графе G_4 завершить при достижении начального состояния z_0 в соответствии с таблицей 4.

Таблица 4

z(t)	z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7
z(t+1) $f_{oc}=0$	(z0)	(z2)	(z4)	(z6)	(z0)	(z2)	z4	(z6)
z(t+1) $f_{oc}=1$	z1	z3	z5	z7	z1	z3	(z5)	z7

На рис. 2 в обобщенном виде представлена граф-схема алгоритма нахождения булевых функций обратных связей *n*-разрядных СРНОС, порождающих последовательности де Брейна в соответствии с представленной выше процедурой.

Возвращаясь к рассматриваемому примеру из таблицы 4 последовательность состояний, образующих гамильтонов цикл в графе G_4 четырехразрядного СР получается в виде: $\delta(z_0,1) = (0001) = z_1^*$, $\delta(z_1,1) = (0011) = z_3^*$, $\delta(z_3,1) = (0111) = z_7^*$, $\delta(z_7,1) = (1111) = z_{15}^*$, $\delta(z_{15},1) = (1110) = z_{14}^*$, и далее $z_{12}^*, z_9^*, z_2^*, z_5^*, z_{11}^*, z_6^*, z_{13}^*, z_{10}^*, z_4^*, z_8^*, z_0^*$ в соответствии с изложенной выше процедурой и алгоритмом.

Если для упрощения записи исключить индексы (*), отличающие состояния графов $G_{(n-1)}$ и G_n, то Гамильтонов цикл в графе G_4, представленный последовательностью состояний $\{z_0, z_1, z_3, z_7, z_{15}, z_{14}, z_{12}, z_9, z_2, z_5, z_{11}, z_6, z_{13}, z_{10}, z_4, z_8, z_0\}$, порождается входной последовательностью

$$P_g = \{0000111100101101000\} \qquad (1)$$

Из последовательности (1) СДНФ функции обратной связи СР определяется в виде:

$$f(x_1, x_2, x_3, x_4) = \sum m(0,1,2,3,5,6,7,12) \qquad (2)$$

где x_i, $i = \overline{1,4}$ – выходы триггеров СР; x_1 – младший разряд.

Минимальная дизъюнктивная нормальная форма функции (2) равна:

$$f_{oc}(x_1, x_2, x_3, x_4) = x_1\overline{x_4} + x_2\overline{x_4} + \overline{x_3}\,\overline{x_4} + \overline{x_1}\,\overline{x_2}x_3x_4 \qquad (3)$$

С целью минимизации аппаратурных затрат и числа соединений в схемной реализации обратных связей предлагается использовать алгоритм синтеза комбинационных схем в виде древовидных структур, что дополнительно обеспечивает синдромную тестируемость комбинационной части генераторов тестов и простоту проверки их исправности [13].

Реализация f_{oc} (2) древовидной схемой представляется булевым выражением:

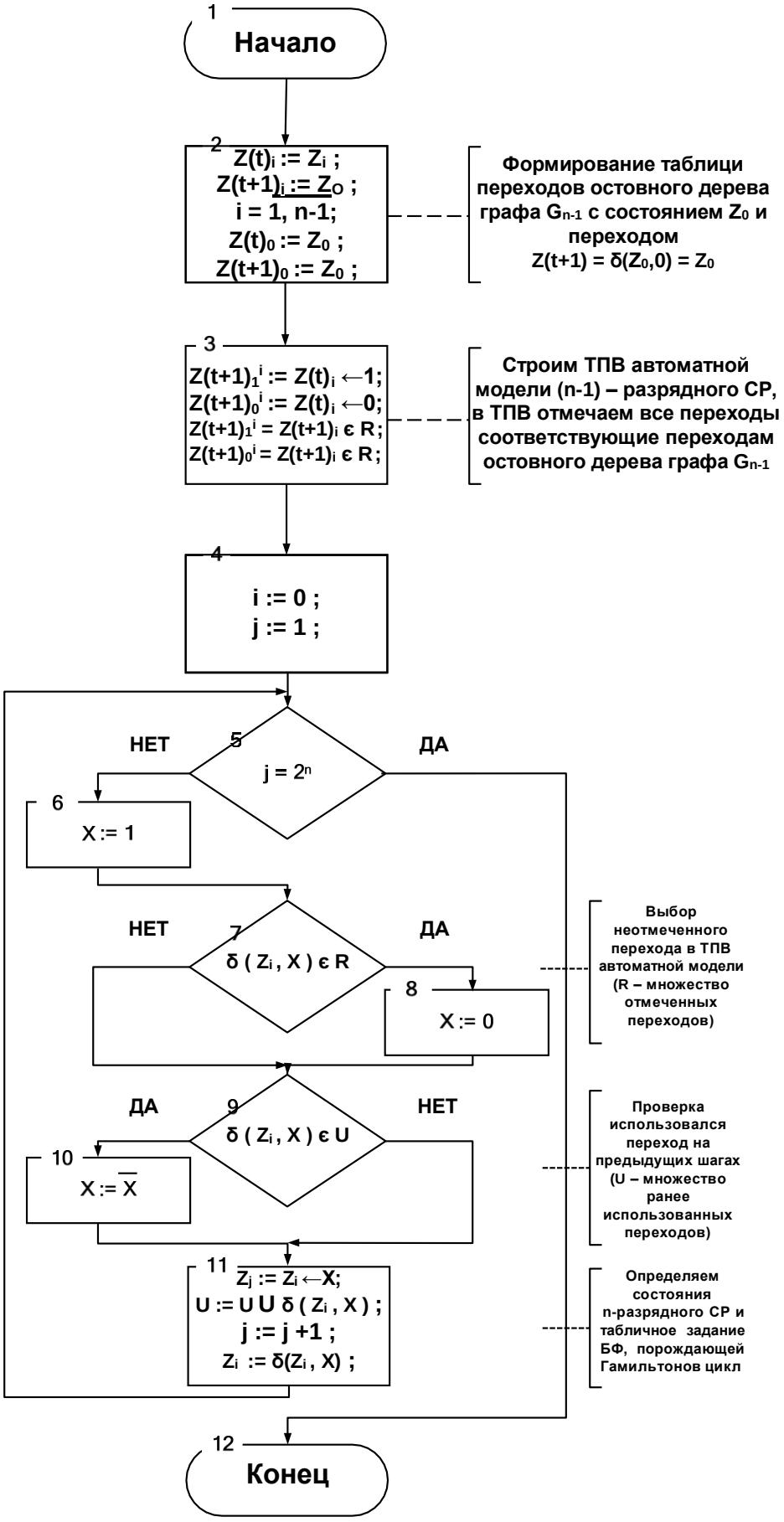


Рисунок 2 – Граф-схема алгоритма нахождения булевых функций, порождающих гамильтоновы циклы в графе *n*-разрядного СР

$$f_{oc}(x_1, x_2, x_3, x_4) = x_4 \oplus \overline{x_1 x_2 x_3} \qquad (4)$$

Затраты на схемную реализацию функций, представленных в виде (3) и (4) следующие:

- реализация по МДНФ – 7,0 в.э, 15 соединений;
- реализация ОС – 3,5 в.э., 6 соединений.

Ниже приведены булевые функции обратных связей СРНОС, соответствующие реализации древовидными схемами всех 16-ти функций f_{oc}, порождающих гамильтоновы циклы в четырёхразрядном СР:

$f_1 = x_4 \oplus (x_3 + \bar{x}_1 \cdot \bar{x}_2)$
$f_2 = x_4 \oplus (\bar{x}_1 + x_2 \cdot x_3)$
$f_3 = x_4 \oplus (\bar{x}_3 + x_1 \cdot x_2)$
$f_4 = x_4 \oplus (x_1 + \bar{x}_2 \cdot \bar{x}_3)$
$f_5 = x_4 \oplus (\overline{(x_1 \oplus x_2)} + x_1 \cdot x_3)$
$f_6 = x_4 \oplus (\overline{(x_1 \oplus x_2)} + \bar{x}_1 \cdot \bar{x}_3)$
$f_7 = x_4 \oplus (\overline{(x_2 \oplus x_3)} + \bar{x}_1 \cdot \bar{x}_3)$
$f_8 = x_4 \oplus (\overline{(x_2 \oplus x_3)} + x_1 \cdot x_3)$
$f_9 = x_4 \oplus (\overline{(x_1 \oplus x_3)} + x_2 \cdot x_3)$
$f_{10} = x_4 \oplus (\overline{(x_1 \oplus x_3)} + \bar{x}_1 \cdot \bar{x}_2)$
$f_{11} = x_4 \oplus (\overline{(x_1 \oplus x_3)} + x_1 \cdot x_2)$
$f_{12} = x_4 \oplus (\overline{(x_1 \oplus x_3)} + \bar{x}_2 \cdot \bar{x}_3)$
$f_{13} = x_4 \oplus \overline{(\bar{x}_1 \cdot x_2 \cdot x_3)}$
$f_{14} = x_4 \oplus \overline{(x_1 \cdot x_2 \cdot \bar{x}_3)}$
$f_{15} = x_4 \oplus \overline{(x_1 \cdot \bar{x}_2 \cdot \bar{x}_3)}$
$f_{16} = x_4 \oplus \overline{(\bar{x}_1 \cdot \bar{x}_2 \cdot x_3)}$

Анализ этих схем показывает, что критерию минимальности аппаратурных затрат в большей степени соответствуют функции f_{13}, f_{14}, f_{15}, f_{16}. Нахождение таких схожих реализаций с ростом числа n разрядов СР осуществляется путем сравнительного анализа вариантов решений и выбора наилучшего.

Выводы. В работе предложен и обоснован метод и алгоритм синтеза генераторов последовательностей де Брейна на СРНОС, позволяющий повысить степень непредсказуемости ключей в криптографических потоковых шифрах. В качестве критерия синтеза использовался критерий минимальности аппаратных затрат на схемную реализацию генераторов. Предложен алгоритм, реализующий рекурсивную процедуру формирования гамильтоновых циклов в графе n-разрядного сдвигового регистра G_n на основе гомоморфного отображения его состояний в граф состояний регистра $G_{(n-1)}$ и использовании автоматных моделей остовных деревьев графов состояний СР.

Список использованных источников

1. Дербунович Л. В. Генераторы ключевых последовательностей в потоковых криптографических шифрах / Л. В. Дербунович, Д. Г. Караман, А. Н. Осипенко // Тезисы докладов на 3-й Международной научно-практической конференции "Інформаційні технології та комп'ютерна інженерія". — ВНТУ, Винница, — 2012. — сс. 138-139.

2. Siegenthaler T. Decrypting a Class of Stream Ciphers Using Ciphertext Only / T. Siegenthaler // IEEE Trans. on Computers, — 1985. — Vol. C-34, No. 1.— pp. 81-85.

3. Дербунович Л. В. Генераторы детерминированных тестов на сдвиговых регистрах с нелинейной обратной связью / Л. В. Дербунович, Д. А. Татаренко, А. В. Клименко // Вестник НТУ "ХПИ", — 2005. — №7 — сс. 58-63.

4. Derbunovich L. Pseudoexaustive TPG Based on Nonlinear Feedback Shift Registers / L. Derbunovich, M. Berezhyna, M. Ryzhshkova , D. Tatarenko // Информационно-управляющие системы на железнодорожном транспорте. — 2005. — №5(55). — сс. 54-58.

5. Built-in Test for VLSI: Pseudorandom techniques. / [Bardell P. H., McAnney W. H., Savir J.]. — New York: John Wiley & Sons, 1987. — 274 p.

6. А.с. 1347167 СССР, МКИ H03 K 3/84. Генератор псевдослучайных чисел: / Л. В. Дербунович, В. Ф. Бохан, И. Г. Либерг (СССР). — №4022981/21; заявл. 07.02.86; опубл. 23.10.87, Бюл. № 39. — 1с.

7. Fredricksen H. A Survey of full length nonlinear shift register cycle algorithms / H. Fredricksen // SIAM Review. — 1982. — Vol. 24, № 2. — pp. 195-221.

8. Ralston A. De Bruijn sequences — a model example of interaction of discrete mathematics and computer science / A. Ralston // Am. Math. Monthly. — 1982. — Vol. 55, №3. — pp. 131-143.

9. Пападимитриу Х. Комбинаторная оптимизация. Алгоритмы и сложность. / Х. Пападимитриу, К. Стайнглиц. — М.: Мир, 1995. — 512 с.

10. Blelloch G. E. NESL: a nested data-parallel language / G. E. Blelloch // Technical report CMU CS-94, — 1994.

11. Lempel A. On homomorphism of the de Bruijn graph and its application to the design of feedback shift registers / A. Lempel // IEEE Trans. on Computers — 1970. — Vol. 19, №12. — pp. 1204-1209.

12. Басакер Р. Конечные графы и сети. / Р. Басакер, Т. Саати — М.: Наука, 1974. — 482 с.

13. Дербунович Л. В., Караман Д. Г., Пащенко Т. Н. Метод синтеза древовидных легко тестируемых логических схем / Л. В. Дербунович, Д. Г. Караман, Т. Н. Пащенко // Вестник НТУ "ХПИ", — №23, — сс. 64-70.

Анотація

ГЕНЕРАТОРИ ПОСЛІДОВНОСТЕЙ ДЕ БРЕЙНА НА ЗСУВНИХ РЕГІСТРАХ З НЕЛІНІЙНИМ ЗВОРОТНІМ ЗВ'ЯЗКОМ

Дербунович Л. В., Караман Д. Г., Осипенко О. М.

Запропоновано метод та алгоритм синтезу генераторів послідовностей де Брейна на ЗРНЗЗ, що дозволяє спростити процедуру синтезу генераторів та скоротити апаратні затрати на їхню реалізацію.

Abstract

DE BRUIJN SEQUENCE GENERATORS ON NON-LINEAR FEEDBACK SHIFT REGISTERS

L. Derbunovich, D. Karaman, A. Osipenko

The method and the algorithm for de Bruijn sequences synthesis on non-linear feedback shift registers (NLFSRs) are presented, which allows to simplify generators synthesis procedure and to reduce hardware costs for their implementation.