4. Mak-Vil'yams, F. Dzh. Teoriya kodov ispravlyayushchikh oshibki [The theory of error-correcting codes] / F. Dzh. Mak-Vil'yams, N. Dzh. A. Sloehn. — Moscow, 1979. — 745 p.
5. Rostovtsev, A.G. Teoreticheskaya kriptografiya [Theoretical cryptography] / A.G. Rostovtsev, E.B. Makhovenko, — St. Petersburg — 2004. — 478 p.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Дмитришин Д.В.

Поступила в редакцию 20 февраля 2013 г.

УДК 004.056.55

Н.А. Барабанов, инженер,
А.В. Соколов, магистр,
Одес. нац. политехн. ун-т

СЛОЖНОСТЬ АППАРАТНОЙ РЕАЛИЗАЦИИ ПОЛНОГО КЛАССА БЕНТ-ФУНКЦИЙ ЧЕТЫРЕХ ПЕРЕМЕННЫХ

М.О. Барабанов, А.В. Соколов. **Складність апаратної реалізації повного класу бент-функцій чотирьох змінних.** Проведена оптимізація апаратної реалізації високонелінійних бент-функцій чотирьох змінних, в рамках чого знайдений клас бент-функцій, оптимальних з точки зору апаратної реалізації, який може бути використаний для завдань поточного шифрування. Розраховані основні криптографічні характеристики знайдених оптимальних бент-функцій, а також завадостійких кодів на їх основі.
Ключові слова: бент-функції, апаратна реалізація, поточне шифрування, коригувальні коди.

Н.А. Барабанов, А.В. Соколов. **Сложность аппаратной реализации полного класса бент-функций четырех переменных.** Проведена оптимизация аппаратной реализации высоконелинейных бент-функций четырех переменных, в рамках чего найден класс бент-функций, оптимальных с точки зрения аппаратной реализации, который может быть использован для задач поточного шифрования. Рассчитаны основные криптографические характеристики найденных оптимальных бент-функций, а также помехоустойчивых кодов на их основе.
Ключевые слова: бент-функции, аппаратная реализация, поточное шифрование, корректирующие коды.

N.A. Barabanov, A.V. Sokolov. **Hardware implementation complexity of a full class of bent functions of four variables.** In this paper the optimization of hardware implementation of highly nonlinear bent functions of 4 variables is proposed, within which we find a class of bent functions that are optimal in terms of hardware implementation, which can be used for tasks of stream encryption. The main cryptographic properties of the found optimal bent functions are estimated, as well as the error-correcting codes based on them are researched.
Keywords: Bent functions, hardware implementation, stream encryption, error-correcting codes.

Решающую роль, определяющую как криптографическую устойчивость, так и быстродействие большинства современных алгоритмов поточного шифрования (ПШ), играют булевы функции [1]. Такие системы обычно построены по принципу модифицированного шифра Вернама, где в качестве ключа используется псевдослучайная последовательность (гамма), которая по заранее оговоренному закону генерируется по определенному алгоритму. Данная гамма Г поразрядно складывается по модулю 2 с битами исходного сообщения p_i, в результате чего формируется криптограмма

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

$$y_i = p_i \oplus \Gamma_i,\ i = \overline{1, L}, \qquad (1)$$

где L — длина исходного сообщения;

$\oplus$ — сумма по $\mathrm{mod}\,2$.

Сложность и свойства закона генерации псевдослучайной последовательности Г с одной стороны определяет ее качество, а стало быть и криптографическую устойчивость алгоритма ПШ в целом, а с другой стороны — сложность его реализации. Для соблюдения принципов диффузии и конфузии шифрования по Шеннону [1] чаще всего ключевая информация используется как некоторое исходное состояние генерации регистров сдвига с линейной обратной связью (РСЛОС), что позволяет добиться хороших статистических характеристик гаммы, реализуя принцип диффузии, однако при этом принцип конфузии реализуется плохо. Для устранения этого недостатка обычно применяют алгоритм ПШ (рис. 1), при котором несколько РСЛОС подключены ко входу блока высоконелинейной булевой бент-функции $f(x_1, x_2, ..., x_n)$, обладающей высокими показателями криптографического качества. При этом алгоритм ПШ преобразует исходное сообщение в шифротекст в соответствии с видом ключа, структурой РСЛОС и применяемой булевой бент-функцией.

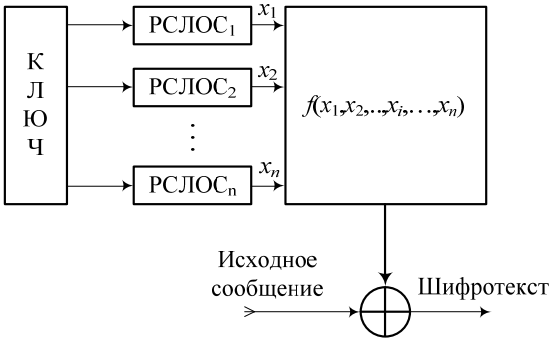

Рис. 1. Алгоритм ПШ на основе РСЛОС и булевой бент-функции

Из анализа работы алгоритма ПШ следует, что его криптографические свойства определяются видом применяемой бент-функции $f(x_1, x_2, ..., x_i, ..., x_n)$, требования к криптографическим характеристикам которых изучены достаточно хорошо [1], однако с точки зрения сложности аппаратной реализации вопросы оптимизации вида данных функций исследованы недостаточно полно. Изучение сложности реализации бент-функций важно при использовании в криптографических алгоритмах их большого количества, т.к. выбор бент-функций, имеющих минимальную аппаратную реализацию, позволяет существенно упростить реализацию алгоритмов ПШ на базе программируемых логических интегральных схем (ПЛИС) [2]. Так, для повышения криптостойкости алгоритма ПШ (см. рисунок 1) можно в качестве рабочей бент-функции выбрать одну из нескольких сотен.

Целью данной статьи является исследование сложности аппаратной реализации полного класса бент-функций от четырех переменных.

Всего булевых функций $n = 4$ переменных существует $J = 2^{2^4} = 65536$, но лишь некоторым из них присущи достаточно хорошие криптографические качества — критерии, делающие возможным их применение в схемах поточного шифрования [1, 3]:

— высокая алгебраическая степень нелинейности $\deg\{f\}$;

— высокое расстояние нелинейности $N_f = \min_j \{\mathrm{dist}(f, \varphi_j)\}$, где $\varphi = \langle a, x \rangle + b$ — кодовые слова аффинного кода, $a, x \in V_n$, $b \in \{0,1\}$; V_n — линейное векторное пространство двоичных векторов длины n;

— соответствие строгому лавинному критерию (strict avalanche criterion — SAC), требующему, чтобы при изменении одного из n входных битов, выходной бит менялся с вероятностью 1/2 [1];

— минимаксный критерий, т.е. минимальный уровень максимального бокового лепестка $R_{\text{ААКФ}}$ и $R_{\text{ПАКФ}}$ соответственно апериодических и периодических автокорреляционных функций (ААКФ и ПАКФ) бент-последовательностей.

Проведенный анализ полного множества булевых функций от $n = 4$ переменных показывает, что наилучшим соответствием всем перечисленным критериям обладают бент-функции [1].

В табл. 1 приведена информация о количестве бент-функций, удовлетворяющих упомянутым критериям.

Таблица 1

Соответствие бент-функций криптографическим критериям качества

Критерий криптографического качества	Мощность класса J	$N_f = \max\{N_f\} = 6$	$\deg\{f\} = 2$	SAC	$R_{\text{ААКФ}} = 3$	$R_{\text{ПАКФ}} = 4$
Количество бент-функций	896	896	896	896	344	832

С другой стороны, при выборе бент-функций для использования в алгоритме ПШ необходимо учитывать сложность их реализации

Под сложностью аппаратной реализации булевой функции будем понимать число элементарных логических элементов (ЛЭ) для ее аппаратной реализации [4]

$$N_{\text{ЛЭ}} = N_{\text{НЕ}} + N_{\text{И}} + N_{\text{ИЛИ}}, \quad (2)$$

где $N_{\text{НЕ}}$, $N_{\text{И}}$, $N_{\text{ИЛИ}}$ — количество элементов ‘‘НЕ’’, ‘И’’ и ‘ИЛИ’’, соответственно, реализующих операции отрицания, конъюнкции и дизъюнкции;

Естественно считать, что число различных ЛЭ для реализации булевой функции равно числу соответствующих операций в записи логического выражения функции.

Для идентификации бент-функций использованы именные четырехразрядные шестнадцатеричные коды, соответствующие записи их таблиц истинности, обозначаемые $\square\square\square\square_h$, где на каждой позиции $\square$ может находиться число от 0 до F.

Вначале рассмотрим прямую реализацию бент-функций с использованием их канонической совершенной дизъюнктивной (СДНФ) или конъюнктивной (СКНФ) нормальной формы [1, 5].

Анализ бент-последовательностей показывает, что половина из них имеет вес Хэмминга $wt_1(f) = 6$, а другая — $wt_2(f) = 10$, что влияет на выбор способа их аппаратной реализации. При $wt_1(f) = 6$ СДНФ бент-функций

$$f_{\text{СДНФ}}(x_1, x_2, x_3, x_4) = \bigvee_{t=0}^{5} K_t, \quad (3)$$

где $\bigvee$ — обозначение операции дизъюнкции;

t — значения из диапазона $i = \overline{0,15}$, на которых $f(x_1, x_2, x_3, x_4) = 1$;

$K_i = \overset{(-)}{x_1} \wedge \overset{(-)}{x_2} \wedge \overset{(-)}{x_3} \wedge \overset{(-)}{x_4}$ — конституента единицы (минтерм) i-го набора переменных, на которых $f(x_1, x_2, x_3, x_4) = 1$;

(—) — обозначение операции отрицания, если переменная, над которой оно стоит, равна нулю.

При $wt_2(f) = 10$ СКНФ бент-функций

$$f_{\text{СКНФ}}(x_1, x_2, x_3, x_4) = \bigwedge_{t=0}^{5} M_t, \quad (4)$$

где t —значения из диапазона $i = \overline{0,15}$, на которых $f(x_1, x_2, x_3, x_4) = 0$;

$\bigwedge$ — обозначение операции конъюнкции;

$M_i = \overset{(-)}{x_1} + \overset{(-)}{x_2} + \overset{(-)}{x_3} + \overset{(-)}{x_4}$ — конституента нуля (макстерм) i-го набора переменных, где $f_{\text{СКНФ}}(x_1, x_2, x_3, x_4) = 0$;

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

(—) — обозначение операции отрицания, если переменная, над которой оно стоит, равна единице.

Анализ бент-функций показал, что для всех функций $N_{\text{НЕ}} = 4$, а сложность реализации бент-функции на основе как СДНФ, так и СКНФ $N_{\text{ЛЭ}} = N_{\text{НЕ}} + N_{\text{И}} + N_{\text{ИЛИ}} = 27$. При этом СДНФ и СКНФ булевых функций избыточны и требуют минимизации путем применения правил склеивания и поглощения термов. Такая минимизация проведена для бент-функций с использованием метода Куайна-Мак-Класки (QMC-метода) [5], который позволяет получить минимальную дизъюнктивную форму (МДФ) функции.

QMC-метод состоит из двух этапов:

— переход от канонической формы (СДНФ или СКНФ) к сокращенной, в рамках чего выполняют операции склеивания и поглощения;

— переход от сокращенной формы к минимальной, происходящий на основе импликантной матрицы [5].

Рассмотрим пример минимальной реализации бент-функции $95\text{C}0_h$, таблица истинности которой

$$f(x_1, x_2, x_3, x_4) = 95\text{C}0_h = [1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0]. \quad (5)$$

Соответственно СДНФ бент-функции

$$f_{\text{СДНФ}}(v) = K_0 + K_3 + K_5 + K_7 + K_8 + K_9 = \overline{\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}}^{\,0} + \overline{\overline{x_1}\,\overline{x_2}\,x_3 x_4}^{\,3} + \overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}^{\,5} + \overline{x_1}\,x_2 x_3 x_4^{\,7} + x_1\overline{\overline{x_2}\,x_3 x_4}^{\,8} + x_1\overline{x_2}\,\overline{x_3}\,\overline{x_4}^{\,9}, \quad (6)$$

где $i = \overline{0,15}$ — номер бита, равного 1 в двоичном векторе.

В результате минимизации с помощью QMC-метода получена МДФ бент-фунцкии

$$f_{\text{МДФ}}(x_1, x_2, x_3, x_4) = x_1\overline{x_2}\,\overline{x_3} + \overline{x_1}x_2x_4 + \overline{x_1}x_3x_4 + \overline{x_2}\,\overline{x_3}\,\overline{x_4}. \quad (7)$$

Схема реализации минимальной бент-функции $95\text{C}0_h$ приведена на рис. 2.

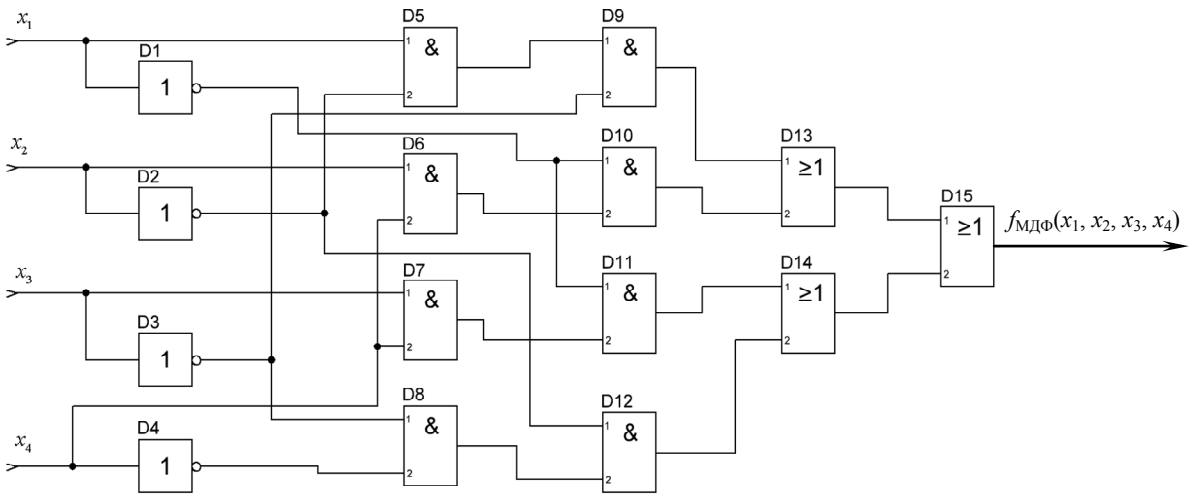

Рис. 2. Схема минимальной реализации бент-функции $95\text{C}0_h$ *: D1…D4 — элементы ‘‘НЕ’’, D5…D12 — элементы ‘‘И’’, D13…15 — элементы ‘‘ИЛИ’’*

В результате анализа МДФ всех 896 бент-функций получены данные о сложности их реализации (табл. 2). Выявлено, что все бент-функции, также как и при использовании СДНФ и СКНФ, требуют для реализации четыре элемента ‘‘НЕ’’ (см. рисунок 2).

Таблица 2

Сложность реализации бент-функций на основе их МДФ

Количество ЛЭ, $N_{ЛЭ}$	15	16	19	21
Количество бент-функций, $N_{БФ}$	288	576	16	16

МДФ бент-функций позволяет сэкономить 6…12 элементов в сравнении с реализацией на основе СДНФ или СКНФ. Анализ данных таблицы 2 показывает, что 288 бент-функций оптимальны с точки зрения минимальной сложности аппаратной реализации. Однако, не все они оптимальны с точки зрения минимаксного критерия боковых лепестков ААКФ и ПАКФ (см. таблицу 1). Только 148 бент-функций оптимальны с точки зрения основных критериев криптографического качества и допускают минимальную сложность аппаратной реализации. Приведены эти булевы функции в виде конструкции, где указанны именные коды бент-функций с минимальной сложностью реализации, при этом жирным шрифтом выделено 80 шестнадцатеричных эквивалентов совершенных двоичных решеток [6],

EBD8	**D7D8**	**EDB8**	**DD78**	BB78	**EBE4**	D7E4	**EEB4**
DE74	**7B74**	**F9AC**	F56C	AF6C	FA9C	5F9C	**F65C**
6F5C	9AFC	**A6FC**	**59FC**	65FC	**B7E2**	**77D2**	BE72
7D72	**9FCA**	F36A	**3F9A**	F63A	**6F3A**	9CFA	39FA
63FA	5FC6	3FA6	**F356**	CF56	F536	AF36	**5CF6**
3AF6	C5F6	**A3F6**	**BE4E**	7D4E	**DE2E**	**7B2E**	**B4EE**
D2EE	**4BEE**	**BB1E**	**74DE**	**2EDE**	**D1DE**	**8BDE**	72BE
4EBE	**B1BE**	8DBE	DDE1	**BBE1**	**DED1**	**7BD1**	**BEB1**
7DB1	AFC9	**F3A9**	CFA9	3F59	FA39	5F39	**ACF9**
53F9	F6C5	**6FC5**	FC65	**3F65**	**9F35**	6CF5	36F5
93F5	BE8D	**7D8D**	EE2D	**772D**	**B8ED**	**47ED**	**B71D**
78DD	1EDD	**87DD**	**727D**	4E7D	B17D	**8D7D**	**F6A3**
6FA3	FA63	F593	**F953**	6AF3	95F3	**DE8B**	**7B8B**
EE4B	774B	D8EB	**E4EB**	**1BEB**	27EB	**EB1B**	D71B
1EBB	**E1BB**	87BB	**747B**	**2E7B**	**D17B**	**8B7B**	**DD87**
ED47	EB27	**D727**	**D8D7**	E4D7	1BD7	**27D7**	**E2B7**
1DB7	B477	**D277**	**2D77**	**6ACF**	56CF	**95CF**	6CAF
36AF	C9AF	5C6F	**3A6F**	**C56F**	A36F	**CA9F**	**359F**
9C5F	C65F	395F	A63F	–	–	–	–

(8)

Для программной реализации практический интерес может представлять реализация бент-функций на основе выражений для их алгебраически нормальной формы (АНФ, полиномов Жегалкина) [1], которые легко реализуются в базисе из элементов ‘‘И’’ и ‘‘Исключающее ИЛИ’’ ($\oplus$). Анализ АНФ всех 896 бент-функций, с точки зрения сложности программной реализации, позволяет построить гистограмму зависимости количества бент-функций $N_{БФ}$ от количества операций $N_{ЛЭ}$ (рис. 3).

Большинство АНФ бент-функций требует 3…10 операций, что существенно меньше, чем для МДФ.

Пример минимальной реализации бент-функции $03A6_h$ на основе АНФ,

$$f(x_1,x_2,x_3,x_4)=03A6_h=[0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0]=x1\wedge x4\oplus x2\wedge x3, \quad (9)$$

обладающей минимальной сложностью реализации АНФ, приведены на рис. 4.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

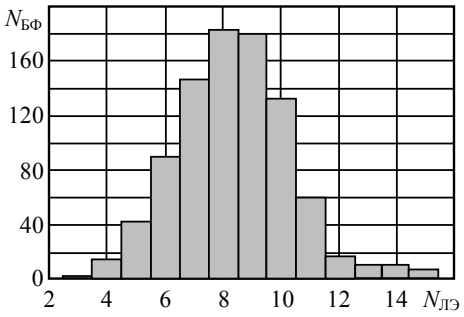

Рис. 3. Гистограмма зависимости количества бент-функций от количества операций в АНФ

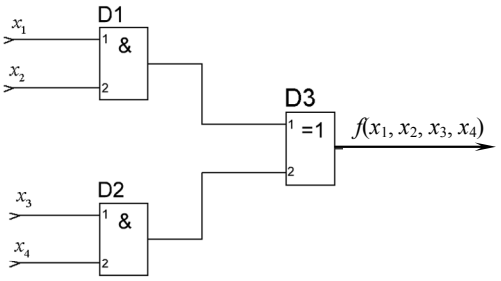

Рис. 4. Схема минимальной реализации АНФ бент-функции $03A6_h$ *на основе, где D3 — элемент ‘‘Исключающее ИЛИ’’*

АНФ в сравнении с МДФ дает беспрецедентно простую реализацию, но только при программной. При аппаратной реализации необходимо учитывать, что операция ‘‘Исключающее ИЛИ’’ —сложная логическая операция, для реализации которой необходимо, по крайней мере, пять элементарных логических элементов. С учетом этого сложность аппаратной реализации бент-функций на основе АНФ приобретает вид $N_{ЛЭ.АНФ} = N_И + 5N_{\oplus}$ [5].

Таким образом, слишком мало бент-функций — 30, имеющих аппаратную реализацию менее, чем 15-ю элементами, однако при очень жестких требованиях к аппаратной части шифровального устройства это также может быть учтено (см. рисунок 3).

Результаты проведенного анализа других приложений бент-функций показывают, что на их базе могут быть построены семейства корректирующих (n, r, d) кодов, где n — длина кодового слова, $r = n - \log_2 J$ — избыточность, d — кодовое расстояние. Представим полученные данные о семействах кодов на основе бент-функций в виде алгебраической конструкции

Мощность класса бент-функции J	896	224	32	4	2
Кодовое расстояние d	4	6	8	10	16

(10)

На основании данных (10) построена сравнительная характеристика семейств корректирующих кодов на основе бент-функций с лучшими из известных корректирующих кодов (табл. 3).

Таблица 3

Сравнительная характеристика семейств корректирующих кодов на основе бент-функций

Ближайшие известные корректирующие коды с меньшим кодовым расстоянием d [7]	Корректирующие коды на основе бент-функций	Ближайшие известные корректирующие коды с бóльшим кодовым расстоянием d [7]
$(16;4,678;3)$	$(16;6,1926;4)$	$(16;8;5)$
$(16;8;5)$	$(16;8,1926;6)$	$(16;10,830;7)$
$(16;10,830;7)$	$(16;11;8)$	$(16;13,415;9)$
$(16;13,415;9)$	$(16;14;10)$	$(16;15;11)$
$(16;15;11)$	$(16;15;16)$	$(19;18;13)$

Анализ показывает, что, обладая минимальной избыточностбю, построенные семейства кодов на основе бент-функций четырех переменных дополняют хорошо известные коды [7].

Основные результаты проведенных исследований:

— получила дальнейшее развитие теория аппаратной реализации бент-функций;

— найден класс бент-функций мощности $J = 144$, оптимальных как с точки зрения минимальной аппаратной реализации, так и по минимаксному критерию;

— проведен анализ программной реализации бент-функций и найдены оценки ее сложности;

— построены семейства корректирующих кодов на основе полного класса бент-функций четырех переменных и показано, что они расширяют известные классы корректирующих кодов, наилучших по критерию минимальной избыточности.

Таким образом, показано, что класс бент-функций является весьма привлекательным для использования в алгоритмах ПШ и теории помехоустойчивого кодирования как по криптографическим и корректирующим свойствам, так и с точки зрения минимальной аппаратной реализации.

Литература

1. Ростовцев, А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. — СПб.: НПО ‘‘ПРОФЕССИОНАЛ’’, 2004. — 478 с.
2. Уэйкерли, Д. Проектирование цифровых устройств / Д. Уэйкерли. — М.: Постмаркет, 2002. — Т.1. — 543 с.
3. Мазурков, М.И. Методы синтеза двоичных псевдослучайных последовательностей со свойством *k*-граммного распределения / М.И. Мазурков, А.В. Соколов // Пр. Одес. політехн. ун-ту. — 2012. — С.188 — 198.
4. Блох, Э.Л. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. — М.: Связь, 1976. — 240 с.
5. Савельев, А.Я. Основы информатики / А.Я. Савельев. — М.: Изд-во МГТУ им. Н.Э. Баумана, 2001. — 328 с.
6. Мазурков, М.И. Класс минимаксных корректирующих кодов на основе совершенных двоичных решеток / М. И. Мазурков // Изв. вузов. Радиоэлектроника. — 2011. — Т. 54, № 9. — С. 24—39.
7. Мак-Вильямс Ф. Д. Теория кодов, исправляющих ошибки / Ф.Д. Мак-Вильямс, Н.Д.А. Слоэн. — М.: Связь. — 1979. — 745 с.

References

1. Rostovtsev, A.G. Teoreticheskaya kriptografiya [Theoretical cryptography] / A.G. Rostovtsev, E.B. Makhovenko // St.Petersburg. — 2004. — 478 p.
2. Ueykerli, D. Proektirovanie tsifrovykh ustroystv [Digital devices design] / D. Ueykerli. — Moscow, 2002. — Vol.1. — 543 p.
3. Mazurkov, M.I. Metody sinteza dvoichnykh psevdosluchaynykh posledovatel’nostey so svoystvom k-grammnogo raspredeleniya [Methods for the synthesis of binary pseudo-random sequences with the property of k-programmatic distribution] / M.I. Mazurkov, A.V. Sokolov. — Odessa: Proceedings of Odessa national polytechnic university. — 2012. — pp.188 — 198.
4. Blokh, E.L. Obobshchennye kaskadnye kody [Generalized cascade codes] / E.L. Blokh, V.V. Zyablov. — Moscow, 1976. — 240 p.
5. Savel’ev, A. Ya. Osnovy informatiki [The foundations of computer science]. — Moscow, 2001. — 328 p.
6. Mazurkov, M.I. Klass minimaksnykh korrektiruyushchikh kodov na osnove sovershennykh dvoichnykh reshetok [The class of minimax error-correcting codes based on the perfect binary arrays] / M.I. Mazurkov // Izvestiya vysshikh uchebnykh zavedeniy. Radioelektronika [News of Higher Schools. Radio engineering]. — 2011. — Vol. 54, # 9. — pp. 24 — 39.
7. Mak-Vil’yams F. D. Teoriya kodov ispravlyayushchikh oshibki [The theory of error-correcting codes] / F. D. Mak-Vil’yams, N. D. A. Sloen // Moscow. — 1979. — 745 p.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Мазурков М.И.

Поступила в редакцию 22 апреля 2013 г.