DOI: 10.21122/2227-1031-2016-15-4-345–352

УДК 681.3.06

Регулярный метод синтеза базовых бент-квадратов произвольного порядка

Канд. техн. наук А. В. Соколов[1)]

[1)]Одесский национальный политехнический университет (Одесса, Украина)

Реферат. Рассматриваются вопросы конструирования классов максимально нелинейных булевых бент-функций произвольной длины $N = 2^k$ (k = 2, 4, 6, …) на основе их спектрального представления – бент-квадратов Агиевича. Данные совершенные алгебраические конструкции являются основой для построения многих криптографических примитивов, таких как генераторы псевдослучайных ключевых последовательностей, криптографические *S*-блоки подстановки и т. д. Бент-функции находят свое применение для построения *C*-кодов в системах с кодовым разделением каналов, которые обладают минимально возможным значением пик-фактора $\kappa = 1$, а также для построения систем ортогональных бифазных сигналов и помехоустойчивых кодов. Все многочисленные применения бент-функций связаны с теорией их синтеза. Однако регулярные методы синтеза полных классов бент-функций произвольной длины $N = 2^k$ в настоящее время неизвестны. В статье предложен регулярный метод синтеза базовых бент-квадратов Агиевича произвольного порядка n на основе регулярного оператора диадного сдвига. Выполнена классификация полного множества спектральных векторов длин (l = 8, 16, …) на основе критерия максимального абсолютного значения и набора абсолютных значений спектральных компонент. Показано, что любой спектральный вектор может быть основой для построения бент-квадрата. Обобщены результаты синтеза бент-квадратов Агиевича порядка n = 8, показано, что существуют только три базовых бент-квадрата для данного порядка, тогда как еще пять могут быть получены с помощью операции ступенчато циклического сдвига. Синтезированы все базовые бент-квадраты порядка n = 16, позволяющие построение бент-функций длиной N = 256. Полученные базовые бент-квадраты могут служить как для непосредственного синтеза бент-функций и их практического использования, так и для проведения дальнейших исследований с целью синтеза новых структур бент-квадратов для порядков n = 16, 32, 64, …

Ключевые слова: бент-функция, бент-квадрат, преобразование Уолша – Адамара, спектральный вектор

Для цитирования: Соколов, А. В. Регулярный метод синтеза базовых бент-квадратов произвольного порядка / А. В. Соколов // *Наука и техника.* 2016. Т. 15, № 4. С. 345–352

Regular Method for Synthesis of Basic Bent-Squares of Random Order

A. V. Sokolov[1)]

[1)]Odessa National Polytechnic University (Odessa, Ukraine)

Abstract. The paper is devoted to the class construction of the most non-linear Boolean bent-functions of any length $N = 2^k$ (k = 2, 4, 6…), on the basis of their spectral representation – Agievich bent squares. These perfect algebraic constructions are used as a basis to build many new cryptographic primitives, such as generators of pseudo-random key sequences, crypto graphic *S*-boxes, etc. Bent-functions also find their application in the construction of *C*-codes in the systems with code division multiple access (CDMA) to provide the lowest possible value of Peak-to-Average Power Ratio (PAPR) $\kappa = 1$, as well as for the construction of error-correcting codes and systems of orthogonal biphasic signals. All the numerous applications of

Адрес для переписки
Соколов Артем Викторович
Одесский национальный политехнический университет
пр. Шевченко, 1,
65044, г. Одесса, Украина
Тел.: +38 048 734-85-21
radiosquid@gmail.com

Address for correspondence
Sokolov Artiom V.
Odessa National Polytechnic University
1 Shevchenko Ave.,
65044, г. Odessa, Ukraine
Tel.: +38 048 734-85-21
radiosquid@gmail.com

bent-functions relate to the theory of their synthesis. However, regular methods for complete class synthesis of bent-functions of any length $N = 2^k$ are currently unknown. The paper proposes a regular synthesis method for the basic Agievich bent squares of any order n, based on a regular operator of dyadic shift. Classification for a complete set of spectral vectors of lengths (l = 8, 16, …) based on a criterion of the maximum absolute value and set of absolute values of spectral components has been carried out in the paper. It has been shown that any spectral vector can be a basis for building bent squares. Results of the synthesis for the Agievich bent squares of order n = 8 have been generalized and it has been revealed that there are only 3 basic bent squares for this order, while the other 5 can be obtained with help the operation of step-cyclic shift. All the basic bent squares of order n = 16 have been synthesized that allows to construct the bent-functions of length N = 256. The obtained basic bent squares can be used either for direct synthesis of bent-functions and their practical application or for further research in order to synthesize new structures of bent squares of orders n = 16, 32, 64, …

Keywords: bent-function, bent-square, Walsh – Hadamard transform, spectral vector

For citation: Sokolov A. V. (2016) Regular Method for Synthesis of Basic Bent-Squares of Random Order. *Science & Technique*. 15 (4), 345–352 (in Russian)

Введение

Бент-функции как эталон нелинейности всего множества булевых функций нашли свое применение в виде основных компонентов многих современных систем передачи и обработки информации. Высокие значения нелинейности булевых бент-функций, а значит, их максимальное удаление от множества аффинных функций обусловливают их широкое использование в современных криптографических алгоритмах [1–3]. Равномерность абсолютных значений спектральных коэффициентов Уолша – Адамара делает бент-функции уникальным классом сигналов для применения в системах с технологией кодового разделения каналов (CDMA – Code Division Multiple Access) с точки зрения снижения пик-фактора передаваемых в системе сигналов до минимально возможного уровня к = 1 [4]. Булевы бент-функции также находят свои многочисленные применения в теории помехоустойчивого кодирования информации, криптоанализа и других областях науки и техники [1].

Со времени открытия бент-функций О. Ротхаусом [5] сегодня можно говорить о вполне сформировавшейся теории бент-функций [1], которая в последние десятилетия получила стремительное развитие. Тем не менее все еще не существует механизмов построения полных классов этих совершенных алгебраических конструкций для произвольного четного числа переменных k. Принимая во внимание крайне высокую непредсказуемость структуры бент-функций, неизвестно, могут ли такие механизмы быть созданы в принципе. Однако для числа переменных k = 4 предложен регулярный метод синтеза полного множества бент-функций на основе специальных опорных матриц [6], тогда как для числа переменных k = 6 предложен метод, основанный на ограниченном переборе в области преобразований Рида – Маллера [7].

Основные положения

Одной из наиболее удачных попыток построения регулярных методов синтеза бент-функций для числа переменных k = 6 является предложенный С. Агиевичем метод, основанный на бент-квадратах. Суть его – классификация полного множества бент-функций на подмножества эквивалентных, относящихся к определенному, соответствующему всему подмножеству, опорному бент-квадрату. Все функции внутри подмножества могут быть синтезированы путем применения к опорному бент-квадрату операций перестановок по строкам и столбцам, а также знаковых кодирований.

Цель настоящей статьи – разработка регулярного метода синтеза базовых бент-квадратов любого наперед заданного порядка n. Определение бент-функций через их спектральные коэффициенты заключается в их представлении в виде экспоненциальной таблицы истинности – бент-последовательности.

Определение 1. Бинарная последовательность $B = [b_0, b_1, \cdots, b_i, \cdots, b_{N-1}]$ (где $b_i \in \{\pm 1\}$, $i = 0, 1, 2, ..., N-1$ – коэффициенты) четной длины $N = 2^k = n^2$ (k = 2, 4, 6, …) называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша – Адамара $W_B(\omega)$, который представим в матричной форме [1, 6]

$$W_B(\omega) = BA_N, \quad \omega = \overline{0, N-1},$$

где A_N – матрица Уолша – Адамара порядка N, которая строится для каждого следующего порядка 2^{L+1} в соответствии с рекуррентным правилом [1]

$$A_{2^{L+1}} = \begin{bmatrix} A_{2^L} & A_{2^L} \\ A_{2^L} & -A_{2^L} \end{bmatrix}.$$

Исходя из определения бент-функций, каждый спектральный коэффициент бент-последовательности $W_B(\omega = 0)$, $W_B(\omega = 1)$, ..., W_B ($\omega = N-1$) принимает значение из множества $\{\pm n\}$, где $n = \sqrt{N}$.

Исследователем С. Агиевичем показано, что для каждой бент-последовательности может быть найден соответствующий бент-квадрат. Бент-квадратом назовем матрицу S порядка n, каждой строкой и каждым столбцом которой является спектральный вектор, полученный в результате умножения сегмента бент-последовательности длины n на матрицу Адамара порядка n [8]

$$S_i = B_i A_n, \quad n = \sqrt{N},$$

где S_i – i-я строка бент-квадрата S; B_i – i-й сегмент бент-последовательности.

В соответствии с эквивалентностью полного множества бент-квадратов, с точки зрения операций перестановок по строкам и столбцам и операции знакового кодирования, среди всех бент-квадратов могут быть выделены восемь базовых структур порядка $n = 8$ [8]

$$S_1 = \begin{bmatrix} 8&0&0&0&0&0&0&0 \\ 0&8&0&0&0&0&0&0 \\ 0&0&8&0&0&0&0&0 \\ 0&0&0&8&0&0&0&0 \\ 0&0&0&0&8&0&0&0 \\ 0&0&0&0&0&8&0&0 \\ 0&0&0&0&0&0&8&0 \\ 0&0&0&0&0&0&0&8 \end{bmatrix}; \quad S_2 = \begin{bmatrix} -4&4&4&4&0&0&0&0 \\ 4&-4&4&4&0&0&0&0 \\ 4&4&-4&4&0&0&0&0 \\ 4&4&4&-4&0&0&0&0 \\ 0&0&0&0&8&0&0&0 \\ 0&0&0&0&0&8&0&0 \\ 0&0&0&0&0&0&8&0 \\ 0&0&0&0&0&0&0&8 \end{bmatrix};$$

$$S_3 = \begin{bmatrix} -4&4&4&4&0&0&0&0 \\ 4&-4&4&4&0&0&0&0 \\ 0&0&-4&4&4&4&0&0 \\ 0&0&4&-4&4&4&0&0 \\ 4&4&0&0&-4&4&0&0 \\ 4&4&0&0&4&-4&0&0 \\ 0&0&0&0&0&0&8&0 \\ 0&0&0&0&0&0&0&8 \end{bmatrix}; \quad S_4 = \begin{bmatrix} -4&4&4&4&0&0&0&0 \\ 4&-4&0&0&4&4&0&0 \\ 4&0&-4&0&4&0&4&0 \\ 4&0&0&-4&0&4&4&0 \\ 0&4&4&0&0&4&-4&0 \\ 0&4&0&4&-4&0&4&0 \\ 0&0&4&4&4&-4&0&0 \\ 0&0&0&0&0&0&0&8 \end{bmatrix};$$

$$S_5 = \begin{bmatrix} -4&4&4&4&0&0&0&0 \\ 4&-4&4&4&0&0&0&0 \\ 4&4&-4&4&0&0&0&0 \\ 4&4&4&-4&0&0&0&0 \\ 0&0&0&0&-4&4&4&4 \\ 0&0&0&0&4&-4&4&4 \\ 0&0&0&0&4&4&-4&4 \\ 0&0&0&0&4&4&4&-4 \end{bmatrix}; \quad S_6 = \begin{bmatrix} -4&4&4&4&0&0&0&0 \\ 4&-4&4&4&0&0&0&0 \\ 0&0&-4&4&4&4&0&0 \\ 0&0&4&-4&4&4&0&0 \\ 0&0&0&0&-4&4&4&4 \\ 0&0&0&0&4&-4&4&4 \\ 4&4&0&0&0&0&-4&4 \\ 4&4&0&0&0&0&4&-4 \end{bmatrix};$$

$$S_7 = \begin{bmatrix} -4&4&4&4&0&0&0&0 \\ 4&-4&0&0&4&4&0&0 \\ 4&0&-4&0&4&0&4&0 \\ 4&0&0&-4&0&4&4&0 \\ 0&4&4&0&-4&0&0&4 \\ 0&4&0&4&0&-4&0&4 \\ 0&0&4&4&0&0&-4&4 \\ 0&0&0&0&4&4&4&-4 \end{bmatrix}; \quad S_8 = \begin{bmatrix} -6&2&2&2&2&2&2&2 \\ 2&-6&2&2&2&2&2&2 \\ 2&2&-6&2&2&2&2&2 \\ 2&2&2&-6&2&2&2&2 \\ 2&2&2&2&-6&2&2&2 \\ 2&2&2&2&2&-6&2&2 \\ 2&2&2&2&2&2&-6&2 \\ 2&2&2&2&2&2&2&-6 \end{bmatrix}. \quad (1)$$

С. Агиевичем также указана возможность построения полного класса бент-последовательностей длины $N = 64$ с помощью операций перестановок по строкам и столбцам и знакового кодирования бент-квадратов (1). Тем не менее методы построения самих бент-квадратов для произвольного порядка n указаны не были.

Для разработки регулярного метода синтеза базовых бент-квадратов рассмотрим классификацию полного множества спектральных векторов. Пусть V_l – линейное векторное пространство векторов υ_i, $i = 0, 1, ..., 2^l - 1$ длины l. Тогда полное множество $J = 2^l$ элементов этого пространства в бинарном виде можно записать

$$V_N = \begin{Bmatrix} + + + + + + ... + \\ + + + + + + ... - \\ . \ . \ . \ . \ . \ . \ . \ . \\ - - - - - - ... - \end{Bmatrix}.$$

Для каждого вектора элемента линейного векторного пространства V_l может быть найден его спектральный вектор путем выполнения преобразования Уолша – Адамара

$$W_i = v_i \cdot A_l.$$

Например, пусть $l = 8$, тогда для вектора элемента линейного векторного пространства V_l $\upsilon_{155} = [- - + - - - + + -]$ спектральный вектор имеет вид $W_{155} = [-2 \ 2 \ -2 \ -6 \ -2 \ 2 \ -2 \ 2]$.

Определение 2 [9]. Элементарной структурой спектрального вектора W_i назовем набор абсолютных значений его спектральных компонент. Например, рассмотренный выше вектор W_{155} имеет элементарную структуру $\{6(1), 2(7)\}$, где

в круглых скобках указано количество раз, которое встречается приведенная спектральная компонента в спектральном векторе.

Определение 3. Параметр $\gamma = \max\{abs(W_i)\}$ спектрального вектора W_i определяется как его максимальное абсолютное значение. Например, вектор W_{155} имеет максимальное абсолютное значение $\gamma_{\max} = 6$. Установлено, что все множество спектральных векторов W_i для каждого значения N может быть разделено на классы в зависимости от элементарной структуры векторов.

Определение 4. Эквивалентным классом спектральных векторов назовем множество таких векторов $\{W_j\}$, каждый из которых имеет одно и то же значение параметра $\gamma_{\max}$ и состоит из одного и того же набора абсолютных значений спектральных компонент. Так, при $l = 8$ множество векторов W_i, $i = 0, 1, ..., 2^8 - 1$ разделяется на три эквивалентных класса (табл. 1).

Таблица 1

Классификация полного множества спектральных векторов W_i длины $l = 8$

Classification for complete set of spectral vectors W_i of length $l = 8$

Номер класса спектральных векторов	Значение параметра $\gamma_{\max} = \max\{abs(W_i)\}$	Набор абсолютных значений спектральных компонент	Объем класса
1	8	$\{\pm 8(1),\ 0(7)\}$	16
2	6	$\{\pm 6(1),\ \pm 2(7)\}$	128
3	4	$\{\pm 4(4),\ 0(4)\}$	112

Выберем из каждого класса по одному спектральному вектору, например:

$$W\begin{bmatrix} W_0 = [8\ 0\ 0\ 0\ 0\ 0\ 0\ 0]; \\ W_{254} = [-6\ 2\ 2\ 2\ 2\ 2\ 2\ 2]; \\ W_{238} = [-4\ 4\ 4\ 4\ 0\ 0\ 0\ 0]. \end{bmatrix} \quad (2)$$

Установлено, что на базе каждого из спектральных векторов (2) возможно построение базового бент-квадрата на основе регулярной операции диадного сдвига.

Определение 5. Две бент-функции называются квадратно-эквивалентными, если бент-квадрат одной из них может быть получен из бент-квадрата другой изменением знаков элементов и перестановкой строк и столбцов.

Определение 6. Базовыми (первичными) бент-квадратами назовем такие, которые строятся прямым методом на основе диадного сдвига и не являются эквивалентными.

Определение 7 [10]. Оператор диадного сдвига представим в виде квадратной матрицы порядка n, которая строится по рекуррентному правилу

$$\mathrm{Diad}(n) = \begin{bmatrix} \mathrm{Diad}(n/2); & \mathrm{Diad}(n/2) + n/2; \\ \mathrm{Diad}(n/2) + n/2; & \mathrm{Diad}(n/2), \end{bmatrix} \quad (3)$$

где $\mathrm{Diad}(2) = \begin{bmatrix} 1, 2 \\ 2, 1 \end{bmatrix}$.

Например, для $n = 8$ в соответствии с (3) получаем

$$\mathrm{Diad}(8) = \begin{bmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 2\,1\,4\,3\,6\,5\,8\,7 \\ 3\,4\,1\,2\,7\,8\,5\,6 \\ 4\,3\,2\,1\,8\,7\,6\,5 \\ 5\,6\,7\,8\,1\,2\,3\,4 \\ 6\,5\,8\,7\,2\,1\,4\,3 \\ 7\,8\,5\,6\,3\,4\,1\,2 \\ 8\,7\,6\,5\,4\,3\,2\,1 \end{bmatrix}. \quad (4)$$

Выполняя с помощью (4) кодирование позиций (индексов) каждого из векторов (2), получаем три базовых бент-квадрата:

$$\mathbb{S}_1^8 = \begin{bmatrix} 80000000 \\ 08000000 \\ 00800000 \\ 00080000 \\ 00008000 \\ 00000800 \\ 00000080 \\ 00000008 \end{bmatrix}; \quad \mathbb{S}_2^8 = \begin{bmatrix} -6\ 2\ 2\ 2\ 2\ 2\ 2\ 2 \\ 2\ -6\ 2\ 2\ 2\ 2\ 2\ 2 \\ 2\ 2\ -6\ 2\ 2\ 2\ 2\ 2 \\ 2\ 2\ 2\ -6\ 2\ 2\ 2\ 2 \\ 2\ 2\ 2\ 2\ -6\ 2\ 2\ 2 \\ 2\ 2\ 2\ 2\ 2\ -6\ 2\ 2 \\ 2\ 2\ 2\ 2\ 2\ 2\ -6\ 2 \\ 2\ 2\ 2\ 2\ 2\ 2\ 2\ -6 \end{bmatrix};$$

$$\mathbb{S}_3^8 = \begin{bmatrix} -4\ 4\ 4\ 4\ 0\ 0\ 0\ 0 \\ 4\ -4\ 4\ 4\ 0\ 0\ 0\ 0 \\ 4\ 4\ -4\ 4\ 0\ 0\ 0\ 0 \\ 4\ 4\ 4\ -4\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ -4\ 4\ 4\ 4 \\ 0\ 0\ 0\ 0\ 4\ -4\ 4\ 4 \\ 0\ 0\ 0\ 0\ 4\ 4\ -4\ 4 \\ 0\ 0\ 0\ 0\ 4\ 4\ 4\ -4 \end{bmatrix},$$

соответствующих S_1, S_8, S_5 из (1). Остальные базовые по С. Агиевичу бент-квадраты могут быть получены из $\mathbb{S}_3^8$ путем знаковых кодирований, перестановок строк, столбцов, ступенчато циклических сдвигов, суперпозиции с сегментами из $\mathbb{S}_1^8$ [8].

Аналогичным образом все множество спектральных векторов W_i, $i = 0, 1, ..., 2^{16} - 1$, длины $l = 16$ можно разделить на восемь эквивалентных классов (табл. 2).

Таблица 2

Классификация полного множества спектральных векторов W_i длины $l = 16$

Classification for complete set of spectral vectors W_i of length $l = 16$

Номер класса спектральных векторов	Значение параметра $\gamma_{\max} = \max\{abs(W_i)\}$	Набор абсолютных значений спектральных компонент	Объем класса
1	16	{16(1), 0(15)}	32
2	14	{14(1), 2(15)}	512
3	12	{12(1), 4(7), 0(8)}	3840
4	10	{10(1), 6(3), 2(12)}	17920
5	8	{8(2), 4(8), 0(6)}	26880
6	8	{8(4), 0(12)}	1120
7	6	{6(6), 2(10)}	14336
8	4	{4(16)}	896

Из каждого эквивалентного класса выберем по одному спектральному вектору:

$$\begin{bmatrix} W_0 = [1600000000000000]; \\ W_{16384} = [14-22222-2-222-2-2-2-222]; \\ W_{257} = [12-4-4-4-4-4-4-4-400000000]; \\ W_{49280} = [1026-26-2-6222-2-2-2-222]; \\ W_{54655} = [-8-8000000-44-44-444-4]; \\ W_{61166} = [-8888000000000000]; \\ W_{63395} = [-62-622-6-6266-2-2-2-2-2-2]; \\ W_{49258} = [444444-4-4-44-44-444-4]. \end{bmatrix} \quad (5)$$

С учетом (3) возможно построить матрицу диадного сдвига для $n = 16$

$$\mathrm{Diad}(16) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 & 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 & 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 & 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\ 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 10 & 9 & 12 & 11 & 14 & 3 & 16 & 15 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 11 & 12 & 9 & 10 & 15 & 16 & 3 & 14 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\ 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 & 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 15 & 16 & 13 & 14 & 11 & 2 & 9 & 10 & 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 16 & 15 & 14 & 13 & 12 & 1 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix},$$

на основе которой для каждого вектора (5) может быть построен соответствующий ему базовый бент-квадрат

$$\begin{cases} \mathbb{S}_1^{16} = W_0(\text{Diad}(16)); \\ \mathbb{S}_2^{16} = W_{16384}(\text{Diad}(16)); \\ \mathbb{S}_3^{16} = W_{257}(\text{Diad}(16)); \\ \mathbb{S}_4^{16} = W_{49280}(\text{Diad}(16)); \\ \mathbb{S}_5^{16} = W_{54655}(\text{Diad}(16)); \\ \mathbb{S}_6^{16} = W_{61166}(\text{Diad}(16)); \\ \mathbb{S}_7^{16} = W_{63395}(\text{Diad}(16)); \\ \mathbb{S}_8^{16} = W_{49258}(\text{Diad}(16)). \end{cases} \qquad (6)$$

Отметим, что бент-квадрат $\mathbb{S}_1^{16}$ представляет собой спектральное отображение конструкции Майорана – МакФарланда [1], которая основана на рекуррентном построении бент-функций на основе перестановок строк и знаковых кодирований матрицы Адамара. Конструкция $\mathbb{S}_1^{16}$ нашла свое применение также и для построения криптографических высоконелинейных *S*-блоков подстановки, которые соответствуют строгому лавинному критерию [11, 12].

Для краткости приведем пример построенного бент-квадрата в виде структуры $\mathbb{S}_3^{16}$:

$$\mathbb{S}_3^{16} = \begin{bmatrix} 12 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 12 & -4 & -4 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & 12 & -4 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & -4 & 12 & -4 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & -4 & -4 & 12 & -4 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & -4 & -4 & -4 & 12 & -4 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & -4 & -4 & -4 & -4 & 12 & -4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & -4 & -4 & -4 & -4 & -4 & -4 & 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & -4 & -4 & -4 & -4 & -4 & -4 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & 12 & -4 & -4 & -4 & -4 & -4 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & 12 & -4 & -4 & -4 & -4 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & 12 & -4 & -4 & -4 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & 12 & -4 & -4 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & -4 & 12 & -4 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & -4 & -4 & 12 & -4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -4 & -4 & -4 & -4 & -4 & -4 & -4 & 12 \end{bmatrix},$$

для которой путем ее матричного произведения над алфавитом $\{\pm 1\}$ с матрицей Адамара A_{16} порядка n = 16 (двумерного преобразования Уолша – Адамара) и последующей конкатенации строк результирующей матрицы получаем бент-последовательность длины N = 256

$$\begin{aligned} B_3 = sign(\mathbb{S}_3^{16} A_{16}) = [& -+++++++-+++++++--+-+-+---+-+-+- \\ & -+--++---+--++-----++--+---++--+ \\ & -+++-----+++------+--+-+--+--+-+ \\ & -+----++-+----++---+-++----+-++- \\ & -++++++++---------+-+-+-++-+-+-+ \\ & -+--++--+-++--++---++--++++--++- \\ & -+++----+---++++--+--+-+++-++-+- \\ & -+----+++-++++-----+-++-+++-+--+]. \end{aligned}$$

Рассмотрим также бент-квадрат $\mathbb{S}_7^{16}$ из (6)

$$\mathbb{S}_7^{16} = \begin{bmatrix} -6 & 2 & -6 & 2 & 2 & -6 & -6 & 2 & 6 & 6 & -2 & -2 & -2 & -2 & -2 & -2 \\ 2 & -6 & 2 & -6 & -6 & 2 & 2 & -6 & 6 & 6 & -2 & -2 & -2 & -2 & -2 & -2 \\ -6 & 2 & -6 & 2 & -6 & 2 & 2 & -6 & -2 & -2 & 6 & 6 & -2 & -2 & -2 & -2 \\ 2 & -6 & 2 & -6 & 2 & -6 & -6 & 2 & -2 & -2 & 6 & 6 & -2 & -2 & -2 & -2 \\ 2 & -6 & -6 & 2 & -6 & 2 & -6 & 2 & -2 & -2 & -2 & -2 & 6 & 6 & -2 & -2 \\ -6 & 2 & 2 & -6 & 2 & -6 & 2 & -6 & -2 & -2 & -2 & -2 & 6 & 6 & -2 & -2 \\ -6 & 2 & 2 & -6 & -6 & 2 & -6 & 2 & -2 & -2 & -2 & -2 & -2 & -2 & 6 & 6 \\ 2 & -6 & -6 & 2 & 2 & -6 & 2 & -6 & -2 & -2 & -2 & -2 & -2 & -2 & 6 & 6 \\ 6 & 6 & -2 & -2 & -2 & -2 & -2 & -2 & -6 & 2 & -6 & 2 & 2 & -6 & -6 & 2 \\ 6 & 6 & -2 & -2 & -2 & -2 & -2 & -2 & 2 & -6 & 2 & -6 & -6 & 2 & 2 & -6 \\ -2 & -2 & 6 & 6 & -2 & -2 & -2 & -2 & -6 & 2 & -6 & 2 & -6 & 2 & 2 & -6 \\ -2 & -2 & 6 & 6 & -2 & -2 & -2 & -2 & 2 & -6 & 2 & -6 & 2 & -6 & -6 & 2 \\ -2 & -2 & -2 & -2 & 6 & 6 & -2 & -2 & 2 & -6 & -6 & 2 & -6 & 2 & -6 & 2 \\ -2 & -2 & -2 & -2 & 6 & 6 & -2 & -2 & -6 & 2 & 2 & -6 & 2 & -6 & 2 & -6 \\ -2 & -2 & -2 & -2 & -2 & -2 & 6 & 6 & -6 & 2 & 2 & -6 & -6 & 2 & -6 & 2 \\ -2 & -2 & -2 & -2 & -2 & -2 & 6 & 6 & 2 & -6 & -6 & 2 & 2 & -6 & 2 & -6 \end{bmatrix},$$

для которого бент-последовательность имеет вид

$$B_7 = [$$
$$\begin{array}{l}
--+++-+----+------++-++++-+---+-+ \\
----+--+--+--+---+-+-++++---+++-++- \\
--++-+-+--+++++-++-------+--+-+-+- \\
-----+---+-+-+---+-+--+-+-++++--+ \\
--+++-+-+++-++++-++-+++++-+++-+-+- \\
----+--+++-++--+-++++--+---+--+-+ \\
--++-+-++++-------++-----+-++-+-+- \\
-----++-++-+--++-+-+--+++----++-].
\end{array}$$

Отметим, что на основе построенных базовых бент-квадратов $\mathbb{S}_1^{16}, ..., \mathbb{S}_8^{16}$ путем применения операций ступенчато циклического сдвига по строкам, суперпозиции сегментов $\mathbb{S}_1^{16}, ..., \mathbb{S}_8^{16}$, операций циклических сдвигов по строкам и столбцам, а также знаковых кодирований может быть получено множество бент-квадратов порядка $n = 16$ и соответственно множество бент-функций длины $N = 256$. Тем не менее разработка регулярных правил построения новых бент-квадратов на основе базовых представляется важной, но все еще нерешенной задачей теории бент-функций.

ВЫВОДЫ

1. Разработан регулярный метод синтеза бент-квадратов С. Агиевича на основе операции диадного сдвига, позволяющий синтезировать базовые бент-квадраты любого порядка n.

2. Дальнейшее развитие получил метод синтеза бент-функций на основе бент-квадратов Агиевича, в рамках чего синтезирован полный класс из восьми базовых бент-квадратов порядка $n = 16$.

3. Предложена классификация полного множества спектральных векторов длины $l = 8, 16$ на основе критерия максимального абсолютного значения и набора абсолютных значений спектральных компонент, что позволило разделить все множество спектральных коэффициентов на эквивалентные классы.

4. Предложенный регулярный метод синтеза базовых бент-квадратов на основе оператора диадного сдвига позволяет расширить область применения метода синтеза бент-функций на основе бент-квадратов Агиевича на бóльшие их длины N, что является необходимым для современных информационных технологий, использующих бент-функции для своего функционирования.

ЛИТЕРАТУРА

1. Токарева, Н. Н. Бент-функции: результаты и приложения: обзор работ / Н. Н. Токарева // Прикладная дискретная математика. 2009. № 1 (3). С. 15–37.
2. Мазурков, М. И. Генератор ключевых последовательностей на основе дуальных пар бент-функций / М. И. Мазурков, Н. А. Барабанов, А. В. Соколов // Труды Одесского политехнического университета. 2013. № 3 (42). С. 150–156.
3. Соколов, А. В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов / А. В. Соколов // Праці Одес. політехн. ун-ту. 2014. № 1 (43). С. 180–186.
4. Paterson, K. G. Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebraic Coding Theory // Sequences and their Applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. P. 46–71.
5. Rothaus, O. S. On “Bent” Functions / O. S. Rothaus // Journal of Combinatorial Theory, Series A. 1976. Vol. 20 No 3. P. 300–305.
6. Мазурков, М. И. Регулярные правила построения полного класса бент-последовательностей длины 16 / М. И. Мазурков, А. В. Соколов // Праці Одес. політехн. ун-ту. 2013. № 2 (41). С. 231–237.
7. Meng, Qingshu. A Novel Algorithm Enumerating Bent Functions / Q. Meng [et al.] // Discrete Mathematics. 2008. Vol. 308, Iss. 23. P. 5576–5584.
8. Agievich, S. V. On the Representation of Bent Functions by Bent Rectangles / S. V. Agievich // Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000). Utrecht, Boston: VSP, 2002. P. 121–135.
9. Соколов, А. В. Алгоритм устранения спектральной эквивалентности компонентных булевых функций *S*-блоков конструкции Ниберг / А. В. Соколов, Н. А. Барабанов // Известия высших учебных заведений. Радиоэлектроника. 2015. Т. 58, № 5. С. 41–49.
10. Мазурков, М. И. Быстрые ортогональные преобразования на основе бент-последовательностей / М. И. Мазурков, А. В. Соколов // Інформатика та математичні методи в моделюванні. 2014. № 1. С. 5–13.
11. Соколов, А. В. Новые методы синтеза нелинейных преобразований современных шифров / А. В. Соколов. Германия: Lap Lambert Academic Publishing, 2015. 100 с.
12. Соколов, А. В. Конструктивный метод синтеза нелинейных *S*-блоков подстановки, соответствующих строгому лавинному критерию / А. В. Соколов // Известия высших учебных заведений. Радиоэлектроника. 2013. Т. 56, № 8. С. 43–52.

Поступила 14.09.2015
Подписана в печать 17.11.2015
Опубликована онлайн 28.07.2016

REFERENCES

1. Tokareva N. N. (2009) Bent-Functions: Results and Applications. Review of Papers. *Prikladnaia Diskretnaia Matematika* [Applied Discrete Mathematics], 3 (1), 15–37 (in Russian).
2. Mazurkov M. I., Barabanov N. A., Sokolov A. V. (2013) Generator of Key Length on the Basis of Bent-Function Dual Pairs. *Pratsi Odes. Politekhn. Un-tu* [Proceedings of Odessa Polytechnical University], 42 (3), 150–156 (in Russian).
3. Sokolov A. V. (2014) Fast-Acting Generator of Key Length on the Basis of Cellular Automaton. *Pratsi Odes. Politekhn*. *Un-tu* [Proceedings of Odessa National Polytechnical University], 43 (1), 180–186 (in Russian).
4. Paterson K. G. (2002) Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebraic Coding Theory. *Proc. SETA 2001 (Discrete Mathematics and Theoretical Computer Science Series)*. Berlin, Springer, 46–71.
5. Rothaus O. S. (1976) On "Bent" Functions. *Journal of Combinatorial Theory, Series A.* 20 (3), 300–305 DOI: 10.1016/0097-3165(76)90024-8
6. Mazurkov M. I., Sokolov A. V. (2013) Regular Rules for Development of Complete Class of Bent-Sequential Length 16. *Pratsi Odes. Politekhn. Un-tu* [Proceedings of Odessa Polytechnical University], 41 (2), 231–237 (in Russian).
7. Qingshu Menga, Min Yangb, Huanguo Zhanga, Jingsong Cuia (2008) A Novel Algorithm Enumerating Bent Functions. *Discrete Mathematics*, 308 (23), 5576–5584 DOI: 10.1016/j.disc.2007.10.024.
8. Agievich S. V. (2002) On the Representation of Bent Functions by Bent Rectangles. *Probabilistic Methods in Discrete Mathematics: Proceedings of the Fifth International Petrozavodsk Conference (Petrozavodsk, June 1–6, 2000)*. Boston: VSP, 121–135.
9. Sokolov A. V., Barabanov N. A. (2015) Algorithm for Removing the Spectral Equivalence of Component Boolean functions of Nyberg-Design S-Boxes. *Radioelectronics and Communications Systems*, 58 (5), 220–227. DOI: 10.3103/S0735272715050040.
10. Mazurkov M. I., Sokolov A. V. (2014) Fast Orthogonal Transformations on the Basis of Bent Sequences. *Informatika ta Matematichni Metodi v Modeliuvanni* [Informatics and Mathematical Methods in Simulation], (1), 5–13 (in Russian).
11. Sokolov A. V. (2015) *New Methods for Synthesis of Non-Linear Transformations in Modern Codes*. Germany, Lap Lambert Academic Publishing. 100.
12. Sokolov A. V. (2013) Constructive Method for the Synthesis of Nonlinear S-Boxes Satisfying the Strict Avalanche Criterion. *Radioelectronics and Communications Systems*, 56 (8), 415–423. DOI: 10.3103/S0735272713080049.

Received: 14.09.2015
Accepted: 17.11.2015
Published online: 28.07.2016