УДК 681.3.06

Методы синтеза бент-матриц

А. В. Соколов

Предложен регулярный метод синтеза полного класса бент-матриц четвертого порядка, основанный на операциях перестановки строк и столбцов, а также построчных циклических сдвигах пяти опорных конструкций. Установлены базовые свойства синтезированного класса бент-матриц, найдена взаимосвязь между полным классом бент-матриц четвертого порядка и классом бент-функций длины $n=16$. Разработан метод построения бесконечных множеств бент-матриц на основе регулярного оператора диадного сдвига.

Ключевые слова: бент-матрица, бент-последовательность, полный класс, криптографический алгоритм, CDMA.

1. Введение

Одной из важнейших характеристик булевых функций, определяющей возможность их применения как в криптографии, так и в теории кодирования, является их нелинейность. Нелинейность булевой функции принято измерять в смысле её расстояния Хэмминга до аффинного кода (кода Рида–Маллера первого порядка). Булевы функции от четного числа переменных, обладающие максимальным расстоянием нелинейности, принято называть бент-функциями, а их таблицы истинности, соответственно, бент-последовательностями. Бент-функции со времени своего открытия [1] получили огромное внимание исследователей, так что в настоящие время можно говорить о сформировавшейся теории бент-функций [2]. Булевы бент-функции обладают практически привлекательными свойствами, такими как наиболее затрудненная аппроксимация множеством аффинных функций, что обуславливает их широкое распространение в блочных и поточных криптографических алгоритмах. Так, в работе [3] предложен алгоритм синтеза криптографических *S*-блоков подстановки, соответствующих как критерию высокой нелинейности, так и строгому лавинному критерию, основанный на применении свойств бент-последовательностей. В работе [4] предложена схема генерации псевдослучайных ключевых последовательностей, основанная на бент-функциях, которая получила свое дальнейшие развитие в [5].

Другое свойство бент-последовательностей — равномерный спектр амплитуд Уолша–Адамара обуславливает их повсеместное применение в технологии CDMA (Code Division Multiple Access), используемой большинством поставщиков беспроводного оборудования в мире согласно стандартам мобильной связи третьего поколения [6].

Столь высокая практическая значимость указанных совершенных алгебраических конструкций диктует необходимость дальнейшего развития методов и алгоритмов их синтеза [7, 8], а также поиска новых конструкций, основанных на бент-функциях, которые могут послужить базисом для усовершенствования существующих криптографических и телекоммуникационных технологий.

В частности, теоретический и практический интерес представляет поиск двумерных аналогов бент-функций по образу синтезированных ранее [9] совершенных двоичных решеток,

которые нашли свои многочисленные применения в современной теории и практике передачи информации.

Целью настоящей статьи является разработка регулярных методов синтеза таких совершенных алгебраических конструкций, как бент-матрицы (двумерные бент-функции).

2. Совершенные алгебраические конструкции — бент-матрицы

Определение 1 [7]. Бинарная последовательность $B=[b_0,b_1,\cdots,b_i,\cdots,b_{n-1}]$ длины n, где $b_i\in\{\pm1\}$ – коэффициенты, $i=\overline{0,n-1}$, $n=2^k$, $k=2,4,6,8,\ldots$, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша–Адамара $W_B(\omega)$, который представим в матричной форме

$$W_B(\omega)=BA,\ \omega=\overline{0,n-1}, \tag{1}$$

где A — матрица Уолша–Адамара размера $n\times n$.

Исходя из определения, каждый спектральный коэффициент $W_B(\omega=0),W_B(\omega=1),\ldots,W_B(\omega=n-1)$ принимает значения из множества $\{\pm2^{k/2}\}$.

Определение 2. Бент-матрицей называется матрица порядка $N=2^k$, $k=2,4,6,8,\ldots$, все строки и столбцы которой являются бент-последовательностями.

Например, приведем матрицу порядка $N=4$, соответствующую **Определению 1** в двоичном и бинарном коде соответственно (элементарное отображение $0\to$"+", $1\to$"–")

$$M_1=\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix}\to\begin{bmatrix}+&+&+&-\\+&+&-&+\\+&-&+&+\\-&+&+&+\end{bmatrix}. \tag{2}$$

Свойство 1. Каждая строка и каждый столбец бент-матрицы обладает максимальным расстоянием нелинейности.

Так, для нашего примера строки и столбцы матрицы (2) представляют собой набор из 4-х булевых бент-последовательностей $\{[+++-],[++-+],[+-++],[-+++]\}$, каждая из которых обладает максимальным расстоянием нелинейности $N_f=1$ среди последовательностей длины $n=4$ и равномерным спектром амплитуд Уолша–Адамара.

Свойство 2. Коэффициенты двумерного преобразования Уолша–Адамара бент-матрицы являются равными по модулю.

Определим двумерное преобразование Уолша–Адамара как

$$\Lambda=M\cdot A, \tag{3}$$

где матрица M представлена в бинарном виде. Так, для нашего примера (2) двумерное преобразование Уолша–Адамара имеет вид

$$\Lambda=\begin{bmatrix}+&+&+&-\\+&+&-&+\\+&-&+&+\\-&+&+&+\end{bmatrix}\begin{bmatrix}+&+&+&+\\+&-&+&-\\+&+&-&-\\+&-&-&+\end{bmatrix}=\begin{bmatrix}2&2&2&-2\\2&-2&2&2\\2&2&-2&2\\2&-2&-2&-2\end{bmatrix}, \tag{4}$$

т.е. все коэффициенты двумерного преобразования Уолша–Адамара являются равными по модулю.

Аналогично классу бент-последовательностей важной с точки зрения практического применения является задача построения полных классов бент-матриц. Экспериментальные исследования показывают, что для порядка матриц $N=4$ существует точно $J_4=512$ бент-матриц.

3. Регулярный метод синтеза полного класса бент-матриц четвертого порядка

В целях облегчения задачи синтеза полного класса бент-матриц регулярными методами введем понятие строковой весовой структуры бент-матрицы.

Определение 3. Строковой весовой структурой бент-матрицы назовем вес строк её двоичного представления (полученного в результате элементарного отображения между бинарным и двоичным кодом $"+"\to 0, "-"\to 1$).

Например, для бент-матрицы (2) строковая весовая структура имеет вид $S_1=[1\ 1\ 1\ 1]^T$. Методом моделирования показано, что полное множество бент-матриц порядка $N=4$ содержит 5 различных строковых весовых структур с точностью до перестановок строк

$$S_1=\begin{bmatrix}1\\1\\1\\1\end{bmatrix},\quad S_2=\begin{bmatrix}1\\1\\1\\3\end{bmatrix},\quad S_3=\begin{bmatrix}1\\1\\3\\3\end{bmatrix},\quad S_4=\begin{bmatrix}1\\3\\3\\3\end{bmatrix},\quad S_5=\begin{bmatrix}3\\3\\3\\3\end{bmatrix}, \tag{5}$$

для каждой из которых может быть выписана матрица-представитель соответствующего структуре класса

$$M_1=\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix},\quad M_2=\begin{bmatrix}0&0&0&1\\1&0&0&0\\1&0&0&0\\1&1&1&0\end{bmatrix},\quad M_3=\begin{bmatrix}0&1&0&0\\1&0&0&0\\1&1&0&1\\1&1&1&0\end{bmatrix},$$
$$M_4=\begin{bmatrix}0&0&0&1\\1&1&1&0\\1&1&1&0\\1&1&1&0\end{bmatrix},\quad M_5=\begin{bmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{bmatrix}. \tag{6}$$

В настоящей работе предложен регулярный метод построения полного класса бент-матриц четвертого порядка во временной области на основе опорных структур (5). Рассмотрим каждую структуру отдельно.

Структура S_1. Матрица M_1 является матрицей-циркулянтом по построению. Таким образом, перестановки строк и столбцов для матрицы M_1 являются эквивалентными друг другу с точки зрения формирования новых матриц. Проведенные исследования показывают, что матрица M_1 допускает все $4!=24$ перестановки по строкам (или по столбцам). Таким образом, полный класс бент-матриц, который соответствует строковой структуре S_1, обладает мощностью $J_1=24$.

Структура S_2. Матрица M_2 может быть подвергнута 12 перестановкам, которые допустимы как по строкам, так и по столбцам, причем пересечения структур не возникает

$$P_r = P_c = \begin{Bmatrix} 1 & 2 & 3 & 4 & \quad 3 & 2 & 1 & 4 & \quad 3 & 1 & 4 & 2 & \quad 4 & 3 & 2 & 1 \\ 1 & 3 & 4 & 2 & \quad 3 & 2 & 4 & 1 & \quad 3 & 4 & 1 & 2 & \quad 4 & 3 & 1 & 2 \\ 1 & 4 & 2 & 3 & \quad 3 & 1 & 2 & 4 & \quad 3 & 4 & 2 & 1 & \quad 4 & 1 & 2 & 3 \end{Bmatrix}. \tag{7}$$

Кроме того, в множестве перестановок (7) существует 4 базовые перестановки по строкам

$$P_{basic} = \begin{bmatrix} 1 & 2 & 3 & 4 & \quad 1 & 4 & 2 & 3 \\ 1 & 3 & 4 & 2 & \quad 4 & 3 & 2 & 1 \end{bmatrix}, \tag{8}$$

на базе которых возможен синтез бент-матриц на основе регулярного оператора построкового циклического сдвига. Каждой из перестановок (8) соответствует бент-матрица, построенная на основе матрицы M_2

$$M_{21} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \quad M_{22} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad M_{23} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad M_{24} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{9}$$

К каждой из приведенных матриц может быть применена операция построкового циклического сдвига вправо со следующими параметрами сдвига строк, определенными для каждой конструкции соответственно

$$\begin{gathered} \xi_{21} = \left\{ \begin{bmatrix} 0 \\ 3 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 2 \\ 3 \end{bmatrix} \right\}, \quad \xi_{22} = \left\{ \begin{bmatrix} 0 \\ 3 \\ 0 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 3 \\ 2 \end{bmatrix} \right\}, \\ \xi_{23} = \left\{ \begin{bmatrix} 0 \\ 0 \\ 3 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \\ 2 \\ 2 \end{bmatrix} \right\}, \quad \xi_{24} = \left\{ \begin{bmatrix} 0 \\ 3 \\ 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ 2 \\ 3 \end{bmatrix} \right\}. \end{gathered} \tag{10}$$

Итого общая мощность класса бент-матриц структуры S_2 составляет $J_2 = 12 \cdot 12 + 4 \cdot 4 = 144 + 16 = 160$ бент-матриц.

Структура S_3. Матрица M_3 может быть подвергнута $J_r = J_c = 4! = 24$ перестановкам по строкам и по столбцам, в результате чего могут быть получены новые $24 \cdot 24 = 576$ бент-матриц структуры S_3, однако оказывается, что не все они являются уникальными. Для получения уникальных структур на основе матрицы M_3 должны использоваться все $J_r = 4! = 24$ перестановки по строкам, а также следующие $J_c = 6$ перестановок по столбцам.

$$P_c = \begin{Bmatrix} 1 & 2 & 3 & 4 & \quad 4 & 3 & 1 & 2 \\ 2 & 4 & 3 & 1 & \quad 4 & 1 & 3 & 2 \\ 2 & 4 & 1 & 3 & \quad 4 & 1 & 2 & 3 \end{Bmatrix}. \tag{11}$$

Таким образом, общее число бент-матриц, соответствующих структуре S_3, достигает $J_3 = 24 \cdot 6 = 144$.

Структура S_4. Для матрицы M_4 могут быть выделены 4 базовые перестановки

$$P_{basic} = \begin{bmatrix} 1 & 2 & 3 & 4 & \quad 2 & 3 & 1 & 4 \\ 2 & 1 & 3 & 4 & \quad 2 & 3 & 4 & 1 \end{bmatrix}, \tag{12}$$

каждой из которых соответствует матрица, полученная путем применения соответствующей перестановки к исходной матрице M_4

$$M_{41}=\begin{bmatrix}0&0&0&1\\1&1&1&0\\1&1&1&0\\1&1&1&0\end{bmatrix},\quad \mathrm{M}_{42}=\begin{bmatrix}1&1&1&0\\0&0&0&1\\1&1&1&0\\1&1&1&0\end{bmatrix},\quad M_{43}=\begin{bmatrix}1&1&1&0\\1&1&1&0\\0&0&0&1\\1&1&1&0\end{bmatrix},\quad M_{44}=\begin{bmatrix}1&1&1&0\\1&1&1&0\\1&1&1&0\\0&0&0&1\end{bmatrix}. \qquad (13)$$

К каждой из приведенных матриц может быть применена операция построкового циклического сдвига вправо со следующими параметрами сдвига строк, одинаковыми для каждой конструкции

$$\xi=\left\{\begin{bmatrix}0\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\0\\1\\1\end{bmatrix},\begin{bmatrix}0\\0\\2\\2\end{bmatrix},\begin{bmatrix}0\\0\\3\\3\end{bmatrix},\begin{bmatrix}0\\1\\0\\1\end{bmatrix},\begin{bmatrix}0\\1\\1\\0\end{bmatrix},\begin{bmatrix}0\\2\\0\\2\end{bmatrix},\begin{bmatrix}0\\2\\2\\0\end{bmatrix},\begin{bmatrix}0\\3\\0\\3\end{bmatrix},\begin{bmatrix}0\\3\\3\\0\end{bmatrix}\right.$$
$$\left\{\begin{bmatrix}1\\0\\0\\1\end{bmatrix},\begin{bmatrix}1\\0\\1\\0\end{bmatrix},\begin{bmatrix}1\\1\\0\\0\end{bmatrix},\begin{bmatrix}1\\1\\1\\1\end{bmatrix},\begin{bmatrix}1\\1\\2\\2\end{bmatrix},\begin{bmatrix}1\\1\\3\\3\end{bmatrix},\begin{bmatrix}1\\2\\1\\2\end{bmatrix},\begin{bmatrix}1\\2\\2\\1\end{bmatrix},\begin{bmatrix}1\\3\\1\\3\end{bmatrix},\begin{bmatrix}1\\3\\3\\1\end{bmatrix}\right.$$
$$\left\{\begin{bmatrix}2\\0\\0\\2\end{bmatrix},\begin{bmatrix}2\\0\\2\\0\end{bmatrix},\begin{bmatrix}2\\1\\1\\2\end{bmatrix},\begin{bmatrix}2\\1\\2\\1\end{bmatrix},\begin{bmatrix}2\\2\\0\\0\end{bmatrix},\begin{bmatrix}2\\2\\1\\1\end{bmatrix},\begin{bmatrix}2\\2\\2\\2\end{bmatrix},\begin{bmatrix}2\\2\\3\\3\end{bmatrix},\begin{bmatrix}2\\3\\2\\3\end{bmatrix},\begin{bmatrix}2\\3\\3\\2\end{bmatrix}\right.$$
$$\left.\left.\begin{bmatrix}3\\0\\0\\3\end{bmatrix},\begin{bmatrix}3\\0\\3\\0\end{bmatrix},\begin{bmatrix}3\\1\\1\\3\end{bmatrix},\begin{bmatrix}3\\1\\3\\1\end{bmatrix},\begin{bmatrix}3\\2\\2\\3\end{bmatrix},\begin{bmatrix}3\\2\\3\\2\end{bmatrix},\begin{bmatrix}3\\3\\0\\0\end{bmatrix},\begin{bmatrix}3\\3\\1\\1\end{bmatrix},\begin{bmatrix}3\\3\\2\\2\end{bmatrix},\begin{bmatrix}3\\3\\3\\3\end{bmatrix}\right\}. \qquad (14)$$

Таким образом, на основе структуры S_4 может быть получен класс из $J_4=4\cdot 40=160$ бент-матриц.

Структура S_5. Матрица M_5 представляет собой матрицу-циркулянт по построению. К матрице M_5 могут быть применены все $4!=24$ перестановки по строкам (или по столбцам). Таким образом, полная мощность класса бент-матриц, которые соответствуют структуре S_5 составляет $J_5=24$.

Суммируя полученные регулярным методом классы бент-матриц, нетрудно вычислить их общее количество

$$J=J_1+J_2+J_3+J_4+J_5=24+160+144+160+24=512, \qquad (15)$$

что может быть подтверждено вычислениями, проведенными переборным методом.

Установлены следующие свойства синтезированного класса бент-матриц четвертого порядка:

Свойство 3. Бент-матрицы структур S_2 и S_4 в результате конкатенации строк образуют бент-последовательности длины $n=16$.

Например, на основе матрицы M_2 путем конкатенации строк и отображения в бинарный код может быть построена бент-последовательность и её спектр Уолша–Адамара

$$B=\{+++-\,-+++-+++-\,-\,-+\};$$
$$S=\{4\ \text{-}4\ \text{-}4\ \text{-}4\ \ 4\ \ 4\ 4\ \text{-}4\ 4\ 4\ 4\ \text{-}4\ \text{-}4\ \ 4\ 4\ 4\}. \qquad (16)$$

Таким образом, полный класс бент-матриц четвертого порядка включает в себя подкласс бент-последовательностей длины $n=16$ мощности $J_{bent}=320$.

Свойство 4. Бент-матрицы структур S_2 и S_4 содержат в себе подмножество из 192 матриц, обладающих идеальной двумерной автокорреляционной функцией – совершенные двоичные решетки [9].

4. Регулярный метод синтеза бент-матриц на основе конструкции Мэйорана–МакФарланда

Отметим, что для потребностей поточного шифрования важной задачей является получение бент-матриц больших порядков для увеличения скорости работы шифров, а также усиления эффекта конфузии. Однако при больших значениях порядка матрицы данная задача не может быть решена методом перебора ввиду стремительного роста возможных вариантов бинарных матриц. При порядке матрицы $N=256$ количество существующих бинарных матриц достигает $J'_{256}=2^{256^2}=2^{65536}$, что является огромной величиной.

В настоящей статье предложен регулярный рекуррентный метод построения бент-матриц, базирующийся на конструкции Мэйорана–МакФарланда и регулярном операторе диадного сдвига.

Сущность конструкции Мэйорана–МакФарланда заключается в конкатенации всех возможных знаковых кодирований и перестановок строк матрицы Адамара. Пусть, например, задана матрица Адамара порядка $k=4$

$$H_4=\begin{bmatrix}+&+&+&+\\+&-&+&-\\+&+&-&-\\+&-&-&+\end{bmatrix}\rightarrow\begin{bmatrix}0&0&0&0\\0&1&0&1\\0&0&1&1\\0&1&1&0\end{bmatrix}, \tag{17}$$

на основе которой путем последовательной конкатенации строк может быть получена бент-последовательность длины $n=16$

$$\begin{aligned}B_{16}=&\left[+\ +\ +\ +\ +\ -\ +\ -\ +\ +\ -\ -\ +\ -\ -\ +\right]\rightarrow\\&\left[0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\right].\end{aligned} \tag{18}$$

Другие бент-последовательности конструкции Мэйорана–МакФарланда длины $n=16$ могут быть получены также на основе (17) путем выполнения операций знакового кодирования и перестановки строк матрицы Адамара; таким образом, полная мощность класса бент-последовательностей конструкции Мэйорана–МакФарланда длины $n=16$ достигает $J_{16MF}=2^4\cdot 4!=384$. В общем случае данная величина растет пропорционально росту порядка исходной матрицы Адамара в соответствии с формулой

$$J_{NMF}=2^{2^{k/2}}\left(2^{k/2}\right)!. \tag{19}$$

Проведенные эмпирические исследования показывают, что на основе каждой бент-последовательности класса Мэйорана–МакФарланда может быть построена бент-матрица при помощи регулярного оператора диадного сдвига.

Матрица $Diad(N)$ диадного сдвига (диадной перестановки) строится по рекуррентному правилу [10]

$$Diad(N)=\begin{bmatrix} Diad(N/2), & Diad(N/2)+N/2 \\ Diad(N/2)+N/2, & Diad(N/2) \end{bmatrix}, \tag{20}$$

где $Diad(2)=\begin{bmatrix}1,2\\2,1\end{bmatrix}$. Например, для значения $N=16$ получаем

$$Diad(16)=\begin{bmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 14 & 13 & 16 & 15 \\
3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 & 11 & 12 & 9 & 10 & 15 & 16 & 13 & 14 \\
4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 & 12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 \\
5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 & 13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 \\
6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 & 14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 \\
7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 & 15 & 16 & 13 & 14 & 11 & 12 & 9 & 10 \\
8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 16 & 15 & 14 & 13 & 12 & 11 & 10 & 9 \\
9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
10 & 9 & 12 & 11 & 14 & 3 & 16 & 15 & 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\
11 & 12 & 9 & 10 & 15 & 16 & 3 & 14 & 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\
12 & 11 & 10 & 9 & 16 & 15 & 14 & 13 & 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \\
13 & 14 & 15 & 16 & 9 & 10 & 11 & 12 & 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\
14 & 13 & 16 & 15 & 10 & 9 & 12 & 11 & 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\
15 & 16 & 13 & 14 & 11 & 2 & 9 & 10 & 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\
16 & 15 & 14 & 13 & 12 & 1 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1
\end{bmatrix}. \tag{21}$$

Осуществляя перестановку элементов бент-последовательности в соответствии с правилами (строками) построения матрицы диадного сдвига $Diad$, получаем новую бент-матрицу. Так, на основе оператора (21) и бент-последовательности (18) получаем бент-матрицу

$$M=\begin{bmatrix}
+&+&+&+&+&-&+&-&+&+&-&-&+&-&-&+ \\
+&+&+&+&-&+&-&+&+&+&-&-&-&+&+&- \\
+&+&+&+&+&-&+&-&-&-&+&+&-&+&+&- \\
+&+&+&+&-&+&-&+&-&-&+&+&+&-&-&+ \\
+&-&+&-&+&+&+&+&+&-&-&+&+&+&-&- \\
-&+&-&+&+&+&+&+&-&+&+&-&+&+&-&- \\
+&-&+&-&+&+&+&+&-&+&+&-&-&-&+&+ \\
-&+&-&+&+&+&+&+&+&-&-&+&-&-&+&+ \\
+&+&-&-&+&-&-&+&+&+&+&+&+&-&+&- \\
+&+&-&-&-&+&+&-&+&+&+&+&-&+&-&+ \\
-&-&+&+&-&+&+&-&+&+&+&+&+&-&+&- \\
-&-&+&+&+&-&-&+&+&+&+&-&+&-&+&+ \\
+&-&-&+&+&+&-&-&+&-&+&-&+&+&+&+ \\
-&+&+&-&+&+&-&-&-&+&-&+&+&+&+&+ \\
-&+&+&-&-&-&+&+&+&-&+&-&+&+&+&+ \\
+&-&-&+&-&-&+&+&-&+&-&+&+&+&+&+
\end{bmatrix}, \tag{22}$$

полностью соответствующую **Определению 1**. Нетрудно убедиться, что с помощью оператора диадного сдвига (20) и конструкции Мэйорана–МакФарланда может быть построена бент-матрица любого порядка N.

5. Выводы

1. Впервые предложен регулярный метод синтеза полного класса бент-матриц четвертого порядка на основе операций перестановки строк и столбцов, а также построкового циклического сдвига.

2. Впервые разработан регулярный метод синтеза бент-матриц на основе конструкции Мэйорана–МакФарланда, а также регулярного оператора диадного сдвига.

3. Дальнейшее развитие получила теория бент-функций, в рамках чего установлены свойства полного класса бент-матриц четвертого порядка, обнаружена их взаимосвязь с классом бент-последовательностей длины $n=16$, а также совершенных двоичных решеток.

Построенный класс бент-матриц может быть использован при конструировании высоконелинейных S-блоков подстановки, в генераторах псевдослучайных ключевых последовательностей и современных телекоммуникационных системах.

Литература

1. *Rothaus O. S.* On “bent” functions. J. Comb. Theory Ser. A. USA: Academic Press Inc, 1976. №20 (3). P. 300–305.
2. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ. Приклад. дискрет. математика. Томск, 2009. Сер. №1 (3). С. 15–37.
3. *Соколов А. В.* Конструктивный метод синтеза нелинейных S-блоков подстановки, соответствующих строгому лавинному критерию. Известия высших учебных заведений. Радиоэлектроника. 2013. Т. 56, № 8. С. 43–52.
4. *Агафонова И. В.* Криптографические свойства нелинейных булевых функций. Семинар по дискрет. гармон. анализу и геометр. моделированию. СПб.: DHA & CAGD, 2007. С. 1–24.
5. *Мазурков М. И., Барабанов Н. А., Соколов А. В.* Генератор ключевых последовательностей на основе дуальных пар бент-функций. Труды Одесского политехнического университета, 2013. Вып. 3 (42). С. 150–156.
6. *Peterson* 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.
7. *Мазурков М. И., Соколов А. В.* Регулярные правила построения полного класса бент-последовательностей длины 16. Труды ОНПУ, 2013. №2 (41). С. 231–237.
8. *Agievich S. V.* 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). Utrecht, Boston: VSP, 2002, P. 121–135.
9. *Мазурков М. И., Чечельницкий В. Я., Мурр П.* Метод защиты информации на основе совершенных двоичных решеток. Известия высших учебных заведений. Радиоэлектроника, 2008. Т. 51, № 11. С. 53–57.
10. *Мазурков М. И., Соколов А. В.* Быстрые ортогональные преобразования на основе бент-последовательностей. Інформатика та математичні методи в моделюванні. Одеса, 2014. № 1. С. 5–13.

Статья поступила в редакцию 12.11.2015;
переработанный вариант – 25.02.2016

Соколов Артём Викторович
к.т.н., старший преподаватель кафедры информационной безопасности Одесского национального политехнического университета (Украина, Одесса, 65044, пр. Шевченко 1), тел. +38 050 492 32 57, e-mail: radiosquid@gmail.com.

Bent matrix synthesis methods

A. Sokolov

A systematic method of full class bent matrix synthesis of fourth order, based on the operations of permutations of rows and columns, as well as row-cyclic shifts of five basic constructions is proposed. The basic properties of the synthesized bent matrices are found, and the relationship between the complete class of bent matrices of fourth order and bent functions class length $n=16$ is determined. A method for constructing the infinite sets of bent matrices based on regular dyadic shift operator is designed.

Keywords: bent matrix, bent sequence, full class, cryptographic algorithm, CDMA.