УДК 510.644

А. В. СОКОЛОВ[1], О. Н. ЖДАНОВ[2]

КЛАСС СОВЕРШЕННЫХ ТРОИЧНЫХ РЕШЕТОК

1Одесский национальный политехнический университет, Одесса, Украина
2Сибирский государственный университет науки и технологий им. академика М. Ф. Решетнева

В настоящее время совершенные алгебраические конструкции успешно применяются для синтеза систем сигналов, конструирования блочных и поточных криптоалгоритмов, для создания генераторов псевдослучайных ключевых последовательностей. Среди совершенных алгебраических конструкций значительное место занимают бент-последовательности и связанный с ними класс совершенных двоичных решеток. Бент-последовательности применяются для построения современных криптографических примитивов, а также для построения кодов постоянной амплитуды (С-кодов), используемых в технологии кодового разделения каналов. В свою очередь, совершенные двоичные решетки используются для построения корректирующих кодов, систем бифазных фазоманипулированных сигналов и многоуровневых криптографических систем. Развитие методов многозначной логики в современных информационных и коммуникационных системах привлекло внимание исследователей к усовершенствованию методов синтеза многозначных бент-последовательностей для задач криптографии и передачи информации. Новые результаты, полученные в области синтеза троичных бент-последовательностей, делают актуальной задачу изучения класса совершенных троичных решеток. В настоящей статье результаты для совершенных двоичных решеток распространяются на трехзначный случай. На основе понятия разбаланса троичной функции введено определение совершенной троичной решетки. Полный класс совершенных троичных решеток третьего порядка получен регулярным методом, минуя перебор. Так, установлено, что класс совершенных троичных решеток является объединением четырех подклассов, в каждом из которых определены соответствующие методы размножения. В работе установлена взаимосвязь между классом троичных бент-последовательностей и классом совершенных троичных решеток. Полученные результаты являются основой для внедрения совершенных троичных решеток в современные криптографические и телекоммуникационные алгоритмы.

Ключевые слова: *многозначная логика, совершенная троичная решетка, бент-последовательность.*

Введение

Развитие методов многозначной логики, происходящее в настоящее время, обуславливает появление новых подходов к криптографической защите информации. Методы многозначной логики представляют интерес и для перспективных квантовых криптоалгоритмов. Так, в работах [1, 2] предложены эффективные алгоритмы генерации псевдослучайных ключевых последовательностей на основе функций многозначной логики. К настоящему времени уже созданы такие криптографические примитивы, как S-блоки подстановки на основе функций многозначной логики, а также работоспособный блочный симметричный криптоалгоритм на их основе [3], в то время как в работе [4] предложен эффективный поточный шифр на основе недвоичных кодов Рида-Соломона.

Дальнейшее развитие криптографических методов, основанных на использовании принципов многозначной логики во многом сопряжено с исследованием совершенных алгебраических конструкций, например, таких как максимально нелинейные бент-последовательности. Теория двоичных бент-последовательностей является достаточно развитой, построению методов синтеза таких последовательностей посвящено немало работ, например, [5–7]. В двоичном случае бент-последовательности являются основой для построения алгоритмов поточного шифрования, а также блоков замен. Еще одним важным классом алгебраических конструкций являются совершенные двоичные решетки (СДР) [8]. В настоящее время они

получили распространение для построения систем бинарных фазоманипулированных сигналов для CDMA технологии и композиционных матричных криптоалгоритмов.

Как нам представляется, для дальнейшего развития криптографических методов будет полезным исследование многозначных, в первую очередь, трехзначных аналогов совершенных алгебраических конструкций.

Исследования [9] позволили установить связь между классом совершенных двоичных решеток четвертого порядка и классом бент-последовательностей практически ценной длины $N = 16$. Так, полный класс совершенных двоичных решеток (СДР) является подмножеством полного класса бент-последовательностей длины $N = 16$, в то время как для больших длин, СДР являются обособленными совершенными алгебраическими конструкциями и их связь с бент-последовательностями на сегодняшний день не установлена.

Определение 1 [10]. Совершенной двоичной решеткой называют двумерную последовательность-матрицу

$$H(N) = \left\| h_{i,j} \right\|, \quad i, j = \overline{0, N-1}, \quad h_{i,j} \in \{-1, 1\}, \quad (1)$$

имеющую двумерную периодическую автокорреляционную функцию – ДПАКФ (Цwo-dimensional periodic autocorrelation function – 2D PACF), элементы которой определяются следующим соотношением

$$R(m,n) = PACF(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+n} = \begin{cases} N^2, \text{ при } m = n = 0, \\ 0, \text{ при других } m \text{ и } n, \end{cases} \quad (2)$$

где $m, n = \overline{0, N-1}$.

Например, легко видеть, что СДР

$$H(4) = \begin{bmatrix} + & + & + & - \\ + & + & + & - \\ + & + & + & - \\ - & - & - & + \end{bmatrix}$$

имеет

$$\left\| R(m,n) \right\| = \begin{bmatrix} 16 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (3)$$

где элементы $H(4)$ представлены в знаковой форме: $-1 \Rightarrow -$, $+1 \Rightarrow +$.

Практическая ценность совершенных двоичных решеток и их связь с повсеместно используемыми бент-последовательностями делают актуальной задачу обобщения данных алгебраических конструкций на многозначный случай.

Целью настоящей статьи является построение метода синтеза полного класса совершенных троичных решеток (СТР) третьего порядка.

Разбаланс функций 3-логики

Решение задачи построения СТР связано с обобщением определения СДР на случай троичной логики. Напомним основные факты для двоичного случая.

Рассмотрим последовательность $B(t)$, $t = 0, 1, ..., N-1$ из N элементов над алфавитом ± 1. Умножая последовательность $B(t)$, $t = 0, 1, ..., N-1$ на матрицу Адамара H порядка N получаем вектор $S(\omega)$, $\omega = 0, 1, ..., N-1$, который называется вектором коэффициентов преобразования Уолша-Адамара

$$S(\omega) = B(t)H, \quad (4)$$

где матрица Адамара формируется по хорошо известному рекуррентному правилу

$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; H_1 = [1]. \quad (5)$$

Приведем полезный для дальнейшего изложения пример. Пусть задан исходный двоичный вектор $B(t) = \{+--\}$ длины $N = 4$. Соответственно, для нахождения $S(\omega)$ мы должны использовать матрицу Адамара порядка $N = 4$

$$H = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix}. \quad (6)$$

Коэффициенты преобразования Уолша-Адамара находятся умножением исходного вектора $B(t)$ на матрицу Уолша-Адамара (все вычисления проводятся над Z_2):

$$W(1) = (+1)(+1) + (-1)(+1) + (-1)(+1) + (-1)(+1) = +1 - 1 - 1 - 1;$$

$$W(2) = (+1)(+1) + (-1)(-1) + (-1)(+1) + (-1)(-1) = +1 + 1 - 1 + 1;$$

$$W(3) = (+1)(+1) + (-1)(+1) + (-1)(-1) + (-1)(-1) = +1 - 1 + 1 + 1;$$

$$W(4) = (+1)(+1) + (-1)(-1) + (-1)(-1) + (-1)(+1) = +1+1+1-1. \quad (7)$$

В результате получаем новый бинарный вектор, для которого находим сумму элементов. Эта сумма является знаковым представлением такой общепринятой [10] в теории совершенных двоичных решеток величины, как *разбаланс*

$$\Delta_{sign} = K^{(+)} - K^{(-)}, \quad (8)$$

где $K^{(+)}$ – количество элементов «+ 1», а $K^{(-)}$ – количество элементов «–1».

Аналогом преобразования Уолша-Адамара для функций многозначной логики является преобразование Виленкина-Крестенсона [11]. Пусть, например, нам задан троичный вектор $t = [z_0 \ \ z_1 \ \ z_2]$, где $z_0 = e^{j0}$, $z_1 = e^{j2\pi/3}$, $z_2 = e^{j4\pi/3}$.

Коэффициенты преобразования Виленкина-Крестенсона могут быть найдены для вектора t по следующей формуле

$$\Omega = tV', \quad (9)$$

где V – матрица Виленкина-Крестенсона порядка N, равного длине вектора t, штрих означает транспонирование.

Правило рекуррентного построения матриц Виленкина-Крестенсона любого порядка $\mu = 3^L$, $L \in N$ представлено в работах [12, 13]

$$V_{3^L} = \begin{bmatrix} V_{3^{L-1}} & V_{3^{L-1}} & V_{3^{L-1}} \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+1\right) \bmod 3 & \left(V_{3^{L-1}}+2\right) \bmod 3 \\ V_{3^{L-1}} & \left(V_{3^{L-1}}+2\right) \bmod 3 & \left(V_{3^{L-1}}+1\right) \bmod 3 \end{bmatrix}. \quad (10)$$

В нашем случае матрица Виленкина-Крестенсона и матрица, комплексно-сопряженная к ней, имеют следующий вид:

$$V_3 = \begin{bmatrix} z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 \\ z_0 & z_2 & z_1 \end{bmatrix}, \ V_3' = \begin{bmatrix} z_0 & z_0 & z_0 \\ z_0 & z_2 & z_1 \\ z_0 & z_1 & z_2 \end{bmatrix}. \quad (11)$$

Рассмотрим процесс вычисления коэффициентов преобразования Виленкина-Крестенсона

$$\begin{aligned} \Omega(1) &= z_0 z_0 + z_0 z_1 + z_0 z_1; \\ \Omega(2) &= z_0 z_0 + z_1 z_1 + z_2 z_1; \\ \Omega(3) &= z_0 z_0 + z_2 z_1 + z_1 z_1. \end{aligned} \quad (12)$$

Заметим, что удобно от мультипликативной группы корней из единицы Γ_3 перейти к изоморфной ей аддитивной группе кольца Z_3 и наоборот.

Рассмотрим обобщение разбаланса на троичный случай. Пусть $|i|$ – количество элементов i.

Определение 2. Значением разбаланса Δ последовательности над алфавитом $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$ назовем величину

$$\Delta(x) = \sqrt{\left(1 \cdot |0| - 0.5\left(|1| + |2|\right)\right)^2 + \left(\frac{\sqrt{3}}{2}|1| - \frac{\sqrt{3}}{2}|2|\right)^2}. \quad (13)$$

Запишем процедуру нахождения абсолютных значений преобразования Виленкина-Крестенсона в терминах наших определений

$$\left|\Omega_i\right| = \Delta(x \cdot vil_i) \quad (14)$$

где vil_i – i-я функция Виленкина-Крестенсона.

Продолжим рассмотрение нашего примера

$$\Omega(1) = \Delta(z_0 z_0, z_0 z_1, z_0 z_1) = \Delta(0,1,1) = \sqrt{(1 \cdot 1 - 0{,}5(2+0))^2 + \left(\frac{\sqrt{3}}{2}2 - \frac{\sqrt{3}}{2}0\right)^2} = \sqrt{3};$$

$$\Omega(2) = \Delta(z_0 z_0, z_1 z_1, z_2 z_1) = \Delta(0,2,0) = \sqrt{(1 \cdot 2 - 0{,}5(0+1))^2 + \left(\frac{\sqrt{3}}{2}0 - \frac{\sqrt{3}}{2}1\right)^2} = \sqrt{\frac{9}{4} + \frac{3}{4}} = \sqrt{3};$$

$$\Omega(3) = \Delta(z_0 z_0, z_2 z_1, z_1 z_1) = \Delta(0,0,2) = \sqrt{(1 \cdot 2 - 0{,}5(0+1))^2 + \left(\frac{\sqrt{3}}{2}0 - \frac{\sqrt{3}}{2}1\right)^2} = \sqrt{\frac{9}{4} + \frac{3}{4}} = \sqrt{3}. \quad (15)$$

Результат полностью совпадает с результатом прямого метода вычисления коэффициентов преобразования Виленкина-Крестенсона.

Аналогично определению ДПАКФ (2), введем следующее определение.

Определение 3. Периодической автокорреляционной p-функцией назовем следующую сумму

$$Kp(m,n) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} h_{i,j} h_{i+m,j+n} (\bmod p), \quad (16)$$

где $m, n = \overline{0, N-1}$.

При $p = 2$ получается классическая двумерная периодическая автокорреляционная функция.

Пример. Рассмотрим троичную бент-последовательность

$$\beta_1 = \{0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 2 \quad 0 \quad 2 \quad 1\}, \quad (17)$$

которую представим в виде матрицы третьего порядка

$$B_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}. \quad (18)$$

Найдем для матрицы (18) соответствующие элементы матрицы $Kp(m,n)$ согласно (16)

$$Kp = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}. \quad (19)$$

Определение 4. Совершенной троичной решеткой (СТР) назовем матрицу, для которой функция $Kp(m,n)$ является постоянной $Kp(m,n) = \text{const}$ при любых значениях сдвига m и n.

В настоящей работе путем экспериментальных исследований установлено, что все существующие троичные бент-последовательности, количество которых равно $J_B = 486$ [14, 15], представленные в виде троичных матриц порядка $N = 3$, обладают равномерной матрицей $Kp(m,n)$, т.е. являются СТР.

Тем не менее существуют и другие СТР, которые не могут быть образованы из бент-последовательностей. Далее представим регулярные методы синтеза полного множества СТР порядка $N = 3$, опишем правила размножения для каждого из трех подмножеств (классов) и определим мощность множества СТР над алфавитом $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$.

Класс 1.

СТР на основе матриц Виленкина-Крестенсона вида

$$PTA_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}. \quad (20)$$

Правило размножения 1.1. СТР класса 1 допускают все возможные знаковые кодирования строк последовательностями длины $N = 3$.

Например, для матрицы (20) умножением каждой строки на соответствующий элемент последовательности $z = [011]$ получаем новую матрицу

$$PTA_1^{`} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}. \quad (21)$$

Всего возможных правил знакового кодирования существует $J_{11} = 3^3 = 27$.

Правило размножения 1.2. СТР класса 1 допускает все возможные перестановки строк, количество которых $J_{12} = 3! = 6$.

Таким образом, общее количестве СТР класса 1, которые могут быть построены с помощью разработанных двух правил размножения, составляет $J_1 = J_{11}J_{12} = 27 \cdot 6 = 162$.

Класс 2.

СТР вида

$$PTA_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix}. \quad (22)$$

Правило размножения 2.1. Представим исходную СТР (22) в обобщенном виде

$$PTA_2 = \begin{bmatrix} \alpha & \alpha & \beta \\ \alpha & \beta & \alpha \\ \alpha & \gamma & \gamma \end{bmatrix}, \quad (23)$$

где коэффициенты α, β, γ различны и принимают значения из множества $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$, количество способов равно $J_{21} = 3! = 6$.

Правило размножения 2.2. Конструкция (23) СТР класса 2 допускает все возможные перестановки строк, которых существует $J_{22} = 3! = 6$.

Правило размножения 2.3. Конструкция СТР класса 2 допускает все возможные циклические сдвиги столбцов, количество сдвигов равно $J_{23} = N = 3$.

Итого, общее количество СТР, которые могут быть построены на основе правил размножения 2.1–2.3, составляет $J_2 = J_{21}J_{22}J_{23} = 6 \cdot 6 \cdot 3 = 108$.

Класс 3.

СТР вида

$$PTA_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 2 & 2 & 0 \end{bmatrix}. \quad (24)$$

Правило размножения 3.1. Представим исходную СТР (24) в обобщенном виде

$$PTA_3 = \begin{bmatrix} \alpha & \alpha & \beta \\ \alpha & \alpha & \beta \\ \gamma & \gamma & \alpha \end{bmatrix}, \quad (25)$$

где коэффициенты α, β, γ могут принимать значения из множества $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$, соответственно, $J_{31} = 3! = 6$ различными способами.

Правило размножения 3.2. Для СТР третьего класса вида (24) допустимы перестановки строк и столбцов из полного множества перестановок, тем не менее, только перестановки вида

$$P = \begin{cases} 1 & 2 & 3; \\ 1 & 3 & 2; \\ 3 & 1 & 2, \end{cases} \qquad (26)$$

не приводят к появлению повторяющихся структур.

Таким образом, общее количество перестановок строк и столбцов равно $J_{32} = 3 \cdot 3 = 9$.

Итого, применяя к СТР третьего класса правила размножения 3.1, 3.2, можно получить $J_3 = J_{31} J_{32} = 6 \cdot 9 = 54$ различных СТР.

Класс 4.

Решетки, состоящие из 4 символов α, 4-х символов β и одного символа γ, где $\alpha, \beta, \gamma \in \{0, 1, 2\}$. Например,

$$PTA_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix}. \qquad (27)$$

Синтез данных решеток происходит следующим образом.

Шаг 1. Рассмотрим матрицу 3-го порядка, заполненную элементами α.

$$\begin{bmatrix} \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha \\ \alpha & \alpha & \alpha \end{bmatrix}. \qquad (28)$$

Шаг 2. Один элемент γ мы можем разместить в ней $C_9^1 = 9$ различными способами. Данный шаг позволяет создать 9 различных матриц.

Шаг 3. Четыре элемента β могут быть размещены $C_8^4 = 70$ различными способами. Данный шаг позволяет создать 70 различных матриц.

Шаг 4. К полученным решеткам прибавить значения из множества $\{0, 1, 2\}$ по mod 3. Данный шаг позволяет создать 3 различные матрицы из одной.

Итого, предложенный метод позволяет сгенерировать $J_4 = 9 \cdot 70 \cdot 3 = 1890$ СТР.

Таким образом, на основе описанных четырех классов СТР может быть построен полный класс мощности $J_{PTA} = J_1 + J_2 + J_3 + J_4 = 162 + 108 + 54 + 1890 = 2214$.

Выводы

Отметим основные результаты проведенных исследований:

1. Введено определение совершенных троичных решеток, которое является обобщением совершенных двоичных решеток на случай троичной логики.

2. Полный класс совершенных троичных решеток третьего порядка построен регулярными методами. Проведена классификация полного множества совершенных троичных решеток на четыре класса и описаны правила размножения для каждого из них.

3. Введено определение разбаланса троичной последовательности, которое может быть использовано как основа дальнейших исследований совершенных алгебраических конструкций многозначной логики.

Отметим, что полученные результаты ставят новые актуальные задачи, среди которых особо выделим следующие:

– нахождение порядков матриц над алфавитом $\{0, 1, 2\} \leftrightarrow \{z_0, z_1, z_2\}$, для которых существуют совершенные троичные решетки;

– разработка рекуррентных методов синтеза совершенных троичных решеток;

– установление связи между классами бент-последовательностей длин L больше 9 и совершенных троичных решеток;

– разработка методов синтеза матриц Виленкина-Крестенсона на основе совершенных троичных решеток;

– разработка методов синтеза сигнальных и криптографических конструкций на основе совершенных троичных решеток.

ЛИТЕРАТУРА

1. **Гнатюк, С. О.** Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань / С. О. Гнатюк, Т. О. Жмурко, В. М. Кінзерявий, Н. А. Сейлова. – Information Technology and Security, 2015. – Т. 3. – № 2(5). – С. 108–116.

2. **Соколов, А. В.** Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций / А. В. Соколов, О. Н. Жданов, Н. А. Барабанов. – Проблемы физики, математики и техники, 2016. – № 1(26). – С. 85–91.

3. **Zhdanov, O. N.** Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O. N. Zhdanov, A. V. Sokolov. – Far East Journal of Electronics and Communications, 2016. – Vol. 16, No. 3. – P. 573–589.

4. **Tao, Wu.** Stream cipher by reed-solomon code / Wu Tao, Wang Ruomei. – Information and Communication Technology Convergence (ICTC), 2017. – P. 422–427.

5. **Токарева, Н. Н.** Бент-функции: результаты и приложения. Обзор работ / Н. Н. Токарева // Приклад. дискрет. математика. – Томск, 2009. – Сер. № 1(3). – С. 15–37.

6. **Mesnager, S.** Several New Infinite Families of Bent Functions and Their Duals / S. Mesnager.— IEEE Transactions on Information Theory, 2014. – Vol. 60. – No. 7. – P. 4397–4407.

7. **Qingshu, Meng.** A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui. – Discrete Mathematics, 2008. – Vol. 308. – Issue 23. – P. 5576–5584.

8. **Kopilovich, L. E.** On perfect binary arrays / L. E. Kopilovich. – Electronics Letters, 1988. —Vol. 24. – No. 9. – P. 566–567.

9. **Мазурков, М. И.** Регулярные привила построения полного класса бент-последовательностей длины 16 / М. И. Мазурков, А. В. Соколов. – Труды ОНПУ. – 2013. – № 2(41). – С. 231–237.

10. **Wild P.** Infinite families of perfect binary arrays / P. Wild. – Electron. Lett, 1988. – Vol. 24. – No. 14. – P. 845–847.

11. **Трахтман, А. М.** Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. – М.: Сов.радио, 1975. – 208 с.

12. **Stankovic, R. S.** Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. – p. 170.

13. **Соколов, А. В.** Методы синтеза алгебраической нормальной формы функций многозначной логики / А. В. Соколов, О. Н. Жданов, А. О. Айвазян. – Системный анализ и прикладная информатика, 2016. – № 1. – С. 69–76.

14. **Мазурков, М.** Метод синтеза бент-последовательностей в базисе Виленкина-Крестенсона / М. И. Мазурков, А. В. Соколов, Н. А. Барабанов // Известия высших учебных заведений. Радиоэлектроника. – 2016. – Т. 59, N 11. – С. 47–55.

15. **Sokolov, A. V.** Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, O. N. Zhdanov. – Journal of Telecommunication, Electronic and Computer Engineering. – Vol. 8. – No. 9. – P. 39–43.

REFERENCES

1. **Hnatiuk, S. O.** Method for quality evaluation of trit pseudorandom sequence to cryptographic applications / S. O. Hnatiuk, T. O. Zhmurko, V. N. Kinzeriavyi, N. A. Seilova. – Information Technology and Security, 2015. – Vol. 3. – No. 2(5). – C. 108–116.

2. **Sokolov, A. V.** Pseudo-random key sequence generator based on triple sets of bent-functions / A. V. Sokolov, O. N. Zhdanov, N. A. Barabanov. – Problems of physics, mathematics and technics, 2016. – No. 1(26). – P. 85–91.

3. **Zhdanov, O. N.** Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O. N. Zhdanov, A. V. Sokolov. – Far East Journal of Electronics and Communications, 2016. – Vol. 16, No. 3. – P. 573–589.

4. **Tao, Wu.** Stream cipher by reed-solomon code / Wu Tao, Wang Ruomei. – Information and Communication Technology Convergence (ICTC), 2017. – P. 422–427.

5. **Tokareva, N. N.** Bent functions: results and applications. Survey of works / N. N. Tokareva. – Applied Discrete Mathematics. – Tomsk, 2009. – Ser. № 1(3). – P. 15–37.

6. **Mesnager, S.** Several New Infinite Families of Bent Functions and Their Duals / S. Mesnager.— IEEE Transactions on Information Theory, 2014. – Vol. 60. – No. 7. – P. 4397–4407.

7. **Qingshu, Meng.** A novel algorithm enumerating bent functions / Qingshu Meng, Min Yang, Huanguo Zhang, Jingsong Cui. – Discrete Mathematics, 2008. – Vol. 308. – Issue 23. – P. 5576–5584.

8. **Kopilovich, L. E.** On perfect binary arrays / L. E. Kopilovich. – Electronics Letters, 1988. —Vol. 24. – No. 9. – P. 566–567.

9. **Mazurkov, M. I.** The regular rules of constructing the complete class of bent-sequences of length 16 / M. I. Mazurkov, A. V. Sokolov. – Proceedings of ONPU, 2013. – No. 2(41). – P.231–237.

10. **Wild P.** Infinite families of perfect binary arrays / P. Wild. – Electron. Lett, 1988. – Vol. 24. – No. 14. – P. 845–847.

11. **Trakhtman, A. M.** Fundamentals of the theory of discrete signals on finite intervals / A. M. Trakhtman, V. A. Trachtman. – Moscow: Sov. radio, 1975. – p. 208.

12. **Stankovic, R. S.** Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. – p. 170.

13. **Sokolov, A. V.** Synthesis methods of algebraic normal form of many-valued logic functions / A. V. Sokolov, O. N. Zhdanov, A. O. Ayvazyan. – System analysis and applied information science, 2016. – No. 1. – P. 69–76.

14. **Mazurkov, M. I.** Synthesis method for bent sequences in the Vilenkin-Chrestenson basis / M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov. – Radioelectronics and Communications Systems, 2016. – Vol. 59. – No. 11. – P. 510–517.

15. **Sokolov, A. V.** Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov, O. N. Zhdanov. – Journal of Telecommunication, Electronic and Computer Engineering. – Vol. 8. – No. 9. – P. 39–43.

Поступила	*После доработки*	*Принята к печати*
20.11.2017	23.02.2018	01.06.2018

Sokolov A. V., Zhdanov O. N.
radiosquid@gmail.com

THE CLASS OF PERFECT TERNARY ARRAYS

In recent decades, perfect algebraic constructions are successfully being use to signal systems synthesis, to construct block and stream cryptographic algorithms, to create pseudo-random sequence generators as well as in many other fields of science and technology. Among perfect algebraic constructions a significant place is occupied by bent-sequences and the class of perfect binary arrays associated with them. Bent-sequences are used for development of modern cryptographic primitives, as well as for constructing constant amplitude codes (C-codes) used in code division multiple access technology. In turn, per-fect binary arrays are used for constructing correction codes, systems of biphase phase-shifted signals and multi-level cryp-tographic systems. The development of methods of many-valued logic in modern information and communication systems has attracted the attention of researchers to the improvement of methods for synthesizing many-valued bent-sequences for cryptog-raphy and information transmission tasks. The new results obtained in the field of the synthesis of ternary bent-sequences, make actual the problem of researching the class of perfect ternary arrays. In this paper we consider the problem of extending the definition of perfect binary arrays to three-valued logic case, as a result of which the definition of a perfect ternary array was introduced on the basis of the determination of the unbalance of the ternary function. A complete class of perfect ternary arrays of the third order is obtained by a regular method, bypassing the search. Thus, it is established that the class of perfect ternary arrays is a union of four subclasses, in each of which the corresponding methods of reproduction are determined. The paper establishes the relationship between the class of ternary bent-sequences and the class of perfect ternary arrays. The obtained results are the basis for the introduction of perfect ternary arrays into modern cryptographic and telecommunication algorithms.

Keywords: *many-valued logic, perfect ternary array, bent-sequence.*

Соколов Артем, кандидат технических наук, старший преподаватель кафедры Информатики и управления защитой информационных систем Одесского национального политехнического университета. Является автором монографии и более 80 научных публикаций. Научные интересы включают в себя методы защиты информации на основе совершенных алгебраических конструкций, методы синтеза алгоритмов шифрования данных и нелинейных S-блоков.

Artem V. Sokolov was born in Odessa, USSR, in 1990. He received a Bachelor (Hons) degree in systems of technical data protection in 2011, Master (Hons) degree in systems of technical data protection and automation of it's processing in 2013 and Ph. D. degree in data protection systems in 2014 from Odessa National Polytechnic University, Odessa, Ukraine.

From 2012 to 2014 he was a Junior Researcher of the Data Security department in Odessa National Polytechnic University. From 2014 to 2017 he was a Senior Lecturer of the Data Security department in Odessa National Polytechnic University. Since 2017 he is a Senior Lecturer of the department of Informatics and control of information systems protection in Odessa National Polytechnic University. He is the author of a book and more than 80 articles. His research interests include data protection methods based on perfect algebraic constructions, nonlinear S-box synthesis methods, and stream encryption algorithms.

A. V. Sokolov awards and honors include: Gold Medal for high achievements in education, Hons Diploma of Winner in Master Competition, 2013; winner of «Information and communication networks» Ukrainian competition of research papers, 2012; Diploma for excellent academic and research activities, 2010.

Жданов Олег Николаевич, доцент кафедры безопасности информационных технологий Сибирского государственного университета науки и технологий им. академика М. Ф. Решетнева. Общее количество публикаций 75.

Сфера научных интересов: системы дифференциальных уравнений в частных производных, являющиеся моделями процессов в механике сплошных сред, защита информации.

Zhdanov Oleg Nikolaevich was born on April 16, 1964. He graduated from Krasnoyarsk State University in 1986. The Ph. D. thesis in mathematical analysis

was defended in 1994. At the moment O. N. Zhdanov is Associate Professor of Informational Technologies subdepartment of Siberian State University of Science and Technology named after Academician M. F. Reshetnev and associate professor of Algebra and mathematical logic department of Siberian Federal university.

O. N. Zhdanov gives the following lecture courses: «Cryptographic methods of information security» (there is a certificate of Institute of Cryptography, Communication and Information Sciences of the corresponding advanced training), «Number-theoretic algorithms of cryptography», «Reliability theory».

The total number of his publications is 75. Eight of them are study guides.

Together with pupils, he developed a key information choice method for realization of block encryption algorithms. Together with Chalkin T. A. he received the copyright certificate on the program complex realizing the choice of key information for data encryption according to the current standard of Russia.

O. N. Zhanov was awarded by a letter of thanks from Legislative Assembly of Krasnoyarsk Krai, a breastplate of the Ministry of Education and Science of the Russian Federation «For development of students research activity».