А. В. Соколов, О. Н. Жданов, Н. А. Барабанов, Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций, *ПФМТ*, 2016, выпуск 1(26), 85–91

ИНФОРМАТИКА

УДК 004.056.55

ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ТРОЙСТВЕННЫХ НАБОРОВ БЕНТ-ФУНКЦИЙ

А.В. Соколов[1], О.Н. Жданов[2], Н.А. Барабанов[1]

[1]*Одесский национальный политехнический университет*
[2]*Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнёва, Красноярск*

PSEUDO-RANDOM KEY SEQUENCE GENERATOR BASED ON TRIPLE SETS OF BENT-FUNCTIONS

A.V. Sokolov[1], O.N. Zhdanov[2], N.A. Barabanov[1]

[1]*Odessa National Polytechnic University*
[2]*M.F. Reshetnev Siberian State Aerospace University, Krasnoyarsk*

Предлагается схема генератора псевдослучайных ключевых последовательностей на основе математического аппарата многозначной логики и тройственных наборов бент-функций. Разработанный генератор обладает высоким уровнем криптографического и стохастического качества и может быть использован в современных телекоммуникационных системах. Построен и классифицирован полный класс 3-бент-последовательностей. Введено понятие троичной алгебраической нормальной формы, разработан быстрый метод её нахождения.

***Ключевые слова**: генератор ключевых последовательностей, многозначная логика, бент-функция, алгоритм поточного шифрования.*

The scheme of multi-valued pseudorandom key sequence generator based on the triple sets of bent-functions is proposed. Designed generator has a high level of cryptographic and stochastic quality and can be used in modern telecommunication systems. The full class of 3-bent-sequences is constructed and classified. The concept of the ternary algebraic normal form is introduced and the fast method for its finding is developed.

***Keywords**: key sequences generator, multi-valued logic, bent-function, stream encryption algorithm.*

Введение

Базовым компонентом современных алгоритмов поточного шифрования (АПШ) являются генераторы псевдослучайных ключевых последовательностей (ГПКП), которые во многом определяют их быстродействие и криптографическую устойчивость. Разработке ГПКП посвящено большое количество работ. На наш взгляд, одним из наиболее перспективных направлений является построение ГПКП на основе совершенных алгебраических конструкций [1]. Использование совершенных алгебраических конструкций позволяет добиться не только оптимальных стохастических свойств ГПКП, но и получить хорошие криптографические свойства генераторов.

Наиболее удобными совершенными алгебраическими конструкциями для построения ГПКП являются бент-функции (их таблицы истинности – бент-последовательности), что обуславливается их максимальным, среди булевых функций, удалением от множества аффинных функций, равномерным спектром амплитуд преобразования Уолша – Адамара. Схема ГПКП на основе множества бент-функций предложена в работе [1], тем не менее, исследования, проведенные в [2], показали её несовершенство в смысле стохастических свойств, в результате чего была предложена схема ГПКП на основе дуальных пар бент-функций, которая удовлетворяет всем базовым стохастическим тестам [3]. Указанная схема ГПКП получила свое дальнейшее развитие в работе [4], благодаря которой удалось существенно повысить быстродействие данной схемы при сохранении стохастических и криптографических свойств генерируемых ею последовательностей.

Хорошо известны эффективные приложения функций многозначной логики для разработки и практической реализации схем защиты информации.

Целью настоящей работы является построение ГПКП на основе троичных бент-последовательностей (3-*бент-последовательностей*).

Алгоритм поточного шифрования представляет собой набор из шести объектов, а именно [5]:

$$[X = \{x_i\}, K = \{k_i\}, Y = \{y_i\}, E, D, \overline{A}],$$

где X – вектор координат x_i открытого текста; K – вектор координат ключа k_i; Y – вектор координат y_i шифротекста; E – множество правил зашифрования; D – множество правил расшифрования; $\overline{A}$ – алфавит, над которым происходит преобразование.

Базовый принцип работы современных АПШ может быть сведен к следующим уравнениям зашифрования и расшифрования

$$\begin{cases} y_i = x_i \underset{q}{\oplus} z_i; \\ x_i = y_i \underset{q}{\oplus} (-z_i); \end{cases} \quad i = \overline{1, L},$$

где z_i – ключевая последовательность, генерируемая ГПКП на основе ключа K; q – мощность применяемого алфавита $\overline{A}$; L – длина исходного сообщения; $\underset{q}{\oplus}$ – операция сложения по модулю q.

Наиболее употребительным является алфавит $\overline{A} = \{0,1\}$, т. е. полагают $q = 2$, тем не менее, развитие систем обработки и передачи информации, в частности, систем радиосвязи [6], определяет актуальность и других значений q для построения АПШ и ГПКП. В настоящей работе мы полагаем $q = 3$.

Для случая $q = 2$ общепринятой схемой ГПКП является схема, основанная на Регистрах Сдвига с Линейной Обратной Связью (РСЛОС) и последующего нелинейного преобразования, позволяющего достичь высокого уровня криптографической стойкости, показанная на рисунке 0.1.

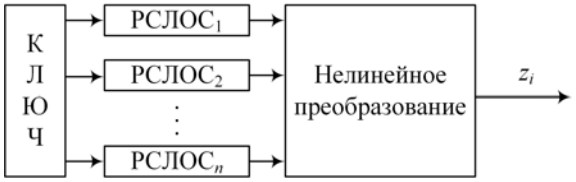

Рисунок 0.1 – Схема ГПКП на основе РСЛОС

В схеме, предложенной в [2], при работе над двоичным алфавитом $\{0,1\}$ в качестве нелинейного преобразования применяются такие совершенные алгебраические конструкции, как дуальные пары бент-последовательностей.

***Определение* 0.1** [7]. Бинарная последовательность

$$B = [b_0, b_1, \cdots, b_i, \cdots, b_{N-1}],$$

длины $N = 2^{2m}$, $m \in \mathbb{N}$, где коэффициенты $b_i \in \{\pm 1\}$, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша – Адамара, который представим в матричной форме

$$|W_B(\omega)| = |B \cdot A_N| = const, \qquad (0.1)$$
$$\omega = \overline{0, N-1},$$

где A_N – матрица Уолша – Адамара порядка N.

Регулярный метод синтеза бент-последовательностей длины $N = 16$ разработан в [8], в то время как метод синтеза бент-последовательностей длины $N = 64$ разработан в [9]. Бент-последовательности бóльших длин могут быть получены с помощью таких рекуррентных конструкций, как конструкция Майорана – МакФарланда [7].

***Определение* 0.2.** Дуальной парой бент-последовательностей называется такой набор из двух бент-последовательностей B_1, B_2, конкатенация таблиц истинности которых $[B_1, B_2]$ является сбалансированной, т. е.

$$K^{-1} = K^{+1} = N.$$

Как показывают исследования, проведенные в работе [2], именно применение дуальных пар бент-последовательностей позволяет добиться наилучших стохастических и криптографических свойств ГПКП.

Разработка ГПКП для случая $q = 3$ требует введения новых видов бент-последовательностей.

Отметим, что свойства бент-последовательности зависят от выбранного ортогонального базиса. В определении 0.1 используется ортогональное преобразование Уолша – Адамара. В свою очередь, каждая строка матрицы Адамара является кодовым словом линейного кода, а, следовательно, постоянные значения трансформант Уолша – Адамара подразумевают, что булева функция включает в себя равные кванты каждой из линейных функций. Это свойство определяет наилучшую криптографическую стойкость бент-последовательностей среди всего множества булевых функций.

Для распространения описанных конструкций на случай $q = 3$ нам понадобятся следующие понятия.

***Определение* 0.3** [10]. Функцией q-значной логики (далее q-функция) k переменных называется отображение

$$\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}.$$

При $q = 2$ получаем булевы функции.

В частности, функция трехзначной логики (3-функция) – это отображение

$$V_k = \{0,1,2\}^k \to \{0,1,2\},$$

т. е. правило, однозначно сопоставляющее вектору из k координат, принимающих значения 0, 1, 2 значение 0, 1 или 2.

Так же, как и булевы функции, 3-функции можно задать аналитически, в виде вектора, в виде таблицы. Важнейшей задачей является определение алгебраической нормальной формы (АНФ) 3-функций.

Пусть 3-функция двух переменных задана таблицей. Для нахождения АНФ данной функции запишем полином:

$$\begin{aligned} f(x_1, x_2) = a_{00} + a_{01}x_2 + a_{02}x_2^{\,2} + \\ + a_{10}x_1 + a_{11}x_1x_2 + a_{12}x_1x_2^{\,2} + \\ + a_{20}x_1^{\,2} + a_{21}x_1^{\,2}x_2 + a_{22}x_1^{\,2}x_2^{\,2}, \end{aligned} \qquad (0.2)$$

где $a_{ij} \in \{0,1,2\}$ – искомые коэффициенты, a_{ij} имеют двойную индексацию: показатель степени первой переменной, показатель степени второй переменной. Например, a_{12} – это коэффициент

при произведении первой степени x_1 и второй степени x_2.

Для поиска коэффициентов a_{ij} составим соответствующую систему уравнений. Для этого подставляем в (0.2) значения переменных и приравниваем заданным значениям многочлена. Решение системы можно записать в виде таблицы 0.1.

Таблица 0.1 – Решение системы

	f_{00}	f_{01}	f_{02}	f_{10}	f_{11}	f_{12}	f_{20}	f_{21}	f_{22}
a_{00}	1	0	0	0	0	0	0	0	0
a_{01}	0	–1	1	0	0	0	0	0	0
a_{02}	–1	–1	–1	0	0	0	0	0	0
a_{10}	0	0	0	–1	0	0	1	0	0
a_{11}	0	0	0	0	1	–1	0	–1	1
a_{12}	0	0	0	1	1	1	–1	–1	–1
a_{20}	–1	0	0	–1	0	0	–1	0	0
a_{21}	0	1	–1	0	1	–1	0	1	–1
a_{22}	1	1	1	1	1	1	1	1	1

Пример. Пусть $k=2$, $x=(x_1,x_2)\in V_2$, 3-функция задана таблицей истинности

x_1	x_2	$f(x)$
0	0	0
0	1	1
0	2	1
1	0	1
1	1	2
1	2	0
2	0	2
2	1	1
2	2	1

Векторное задание этой функции с помощью таблицы истинности: $f(x)=\{011120211\}$. По таблице 0.1 сразу определяем коэффициенты АНФ для нашего примера:

$$a_{ij}=\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} \\ 0 & 0 & 1 & 1 & 2 & 2 & 0 & 2 & 0 \end{bmatrix}^T.$$

Таким образом, с учетом найденных коэффициентов можем записать АНФ исследуемой 3-функции:

$$\Phi(x_1,x_2)=x_1+x_2^2+2x_1x_2+2x_1x_2^2+2x_1^2x_2.$$

Проведем проверку:

$$\Phi(0,0)=0;\ \Phi(0,1)=1;$$
$$\Phi(0,2)=1;\ \Phi(1,0)=1;$$
$$\Phi(1,1)=2;\ \Phi(1,2)=0;$$
$$\Phi(2,0)=2;\ \Phi(2,1)=1;$$
$$\Phi(2,2)=1,$$

что подтверждает правильность вычисленной АНФ.

Отметим, что исследование особенностей структуры найденной матрицы преобразования, а также возможностей её обобщения для другого количества переменных 3-функций является важной задачей, которая все еще ожидает своего решения.

1 Троичные бент-последовательности

Основываясь на понятии алгебраической нормальной формы 3-функции, можем теперь определить 3-аффинный код по аналогии с двоичным аффинным кодом.

***Определение* 1.1.** *Аффинной* называется q-функция аналитического вида

$$\varphi(x_0,\ldots,x_{k-1})=$$
$$=a_0x_0+a_1x_1+\ldots+a_{k-1}x_{k-1}+b(\mathrm{mod}\,q)=$$
$$=\sum_{i=0}^{k-1}a_ix_i+b(\mathrm{mod}\,q),$$

где $a_0,a_1,...,a_{k-1},b\in\{0,1,...,q-1\}$; x_i может принимать значение 0, 1,…, $q-1$.

Единственным отличием общего аналитического вида аффинных функций от линейных является наличие свободного члена *b*, при этом если $b=0$, то функция является линейной. Множество всех аффинных функций от k переменных обозначим A_k.

Например, для случая $k=2$ могут быть выписаны все аффинные функции

$$A_3=\begin{Bmatrix} 000000000 & 111111111 & 222222222 \\ 012012012 & 120120120 & 201201201 \\ 021021021 & 102102102 & 210210210 \\ 000111222 & 111222000 & 222000111 \\ 012120201 & 120201012 & 201012120 \\ 021102210 & 102210021 & 210021102 \\ 000222111 & 111000222 & 222111000 \\ 012201120 & 120012201 & 201120012 \\ 021210102 & 102021210 & 210102021 \end{Bmatrix}.$$

По аналогии с двоичным случаем, на основе линейной части аффинного кода A_3 и отображения

$$0\to e^{j0^\circ},$$
$$1\to e^{j120^\circ},$$
$$2\to e^{j240^\circ}=e^{-j120^\circ},$$

где $j=\sqrt{-1}$, построим ортогональную матрицу, каждая строка которой представляет собой функцию Виленкина – Крестенсона, обобщение матрицы Адамара на трехзначный случай:

$$V=\begin{bmatrix} e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} \\ e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} \\ e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} \\ e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j240^\circ} \\ e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} \\ e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} \\ e^{j0^\circ} & e^{j0^\circ} & e^{j0^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j120^\circ} \\ e^{j0^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j240^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j0^\circ} \\ e^{j0^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j240^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j120^\circ} & e^{j0^\circ} & e^{j240^\circ} \end{bmatrix}.$$

***Определение* 1.2** [11]. Троичная последовательность $H=[h_0,h_1,\cdots,h_i,\cdots,h_{N-1}]$ длины $N=3^{2m}$, $m\in\mathbb{N}$, где коэффициенты $h_i\in\left\{e^{j0^\circ},e^{j120^\circ},e^{j240^\circ}\right\}$, называется 3-бент-последовательностью, если она имеет равномерный по модулю спектр Виленкина – Крестенсона, который представим в матричной форме

$$\Omega_B(\omega)=\left|H\cdot V_N\right|=const,\quad \omega=\overline{0,N-1}, \qquad (1.1)$$

где V_N – матрица Виленкина – Крестенсона порядка N.

Результаты вычислительных экспериментов таковы: существует 486 оптимальных последовательностей длины $N=3^2=9$, удовлетворяющих свойству (1.1), являющихся 3-бент-последовательностями относительно преобразования Виленкина – Крестенсона [12].

Подробный анализ полного класса данных оптимальных последовательностей позволил провести их классификацию: они могут быть разделены на шесть подмножеств

K_0	K_1	K_2	(J_i)
1	4	4	(54);
2	2	5	(108);
2	5	2	(108);
4	1	4	(54);
4	4	1	(54);
5	2	2	(108),

(1.2)

где K_0,K_1,K_2 – количество 0, 1, 2 в троичной последовательности соответственно, с учетом однозначного отображения

$$0\to e^{j0^\circ},1\to e^{j120^\circ},2\to e^{j240^\circ}=e^{-j120^\circ};$$

J_i – количество последовательностей с заданной структурой.

***Определение* 1.3.** Набор из трех 3-бент-последовательностей называется тройственным набором, если конкатенация его таблиц истинности является сбалансированной, т. е.

$$K^0=K^1=K^2.$$

Анализ (1.2) приводит к выводу, что тройственный набор 3-бент-последовательностей может быть составлен двумя различными способами, на основе множества структур

$$\left\{\{1,4,4\},\{4,1,4\},\{4,4,1\}\right\}$$

и $\left\{\{5,2,2\},\{2,5,2\},\{2,2,5\}\right\}$.

2 ГПКП на основе тройственных наборов бент-последовательностей

Предлагается схема ГПКП, основанная на свойствах полного класса 3-бент-последовательностей, разделенного на 2 типа тройственных наборов (рисунок 2.1).

Схема ГПКП на основе тройственных наборов 3-бент-последовательностей, представленная на рисунке 2.1, состоит из двух троичных 3РСЛОС, которые генерируют входные значения для 3-бент-последовательности, а также одного 3РСЛОС, который производит выбор 3-бент-последовательности внутри тройственного набора. Схема содержит один двоичный РСЛОС, который на каждом такте производит выбор одного из двух возможных тройственных наборов (1.2).

Структуры соответствующих РСЛОС полностью определяются неприводимыми первообразными полиномами. Для двоичного случая неприводимые первообразные полиномы можно найти в [13], тогда как полные множества неприводимых W и первообразных неприводимых V полиномов степеней $\deg(p(x))=2,3,...,7$ приведены в таблице 2.1, жирным шрифтом выделены первообразные полиномы.

Рассмотрим более подробно принципы работы разработанного ГПКП поясняя их конкретным примером. Пусть заданы 2 тройственных набора 3-бент-последовательностей

$$\begin{bmatrix} \text{БФ}_1=[011122122]; \\ \text{БФ}_2=[001022202]; \\ \text{БФ}_3=[001001112]; \end{bmatrix} \quad \begin{bmatrix} \text{БФ}_4=[002122212]; \\ \text{БФ}_5=[001112112]; \\ \text{БФ}_6=[000012021], \end{bmatrix}$$

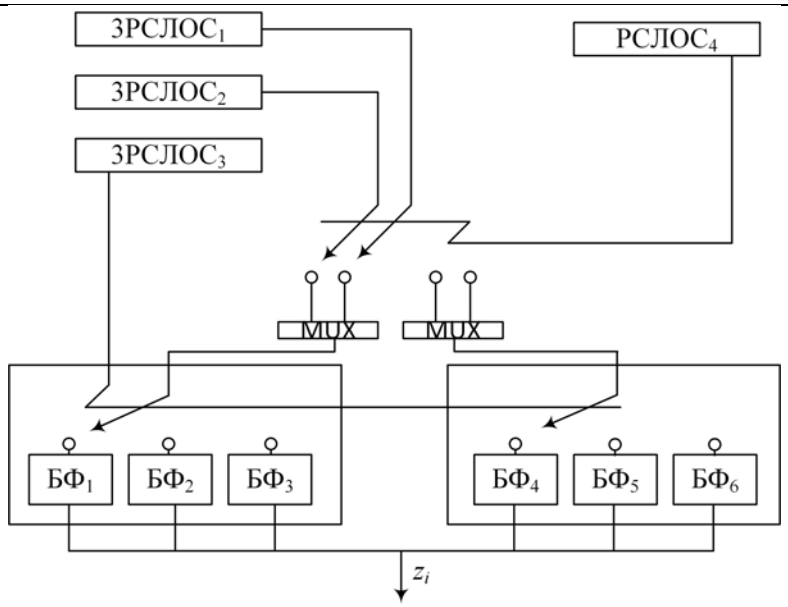

Рисунок 2.1 – ГПКП на основе тройственных наборов 3-бент-последовательностей

Таблица 2.1 – Неприводимые и первообразные полиномы в полях Галуа $GF(3^k)$

Поле	$\|W\|$	$\|V\|$	W, V
$GF(9)$	3	2	10, **14**, **17**
$GF(27)$	8	4	**34**, 35, 38, 41, **43**, **46**, **49**, 53
$GF(81)$	18	8	**86**, **89**, 92, 94, 97, 101, **110**, 115, 118, 121, **125**, **134**, **137**, 139, 145, **149**, 151, **158**
$GF(243)$	48	22	**250**, 251, 257, **265**, **274**, 275, 281, 287, **289**, **295**, **307**, 311, 314, 317, **319**, 322, 326, 329, **331**, **334**, **337**, 341, **355**, **367**, **373**, 374, **379**, 386, 389, **391**, **397**, 398, **406**, **409**, 413, 425, 428, **430**, 437, **445**, 446, 458, 461, **466**, **469**, 470, 478, 482
$GF(729)$	116	48	**734**, **737**, 742, 745, 748, **761**, 763, 766, 773, 781, 787, **791**, 793, 797, 805, 829, **833**, **836**, 838, 841, **845**, **854**, 865, **869**, 871, **878**, 892, 901, **905**, **908**, 925, 929, **932**, 934, 949, 956, 958, **962**, **974**, 977, 985, **1001**, 1003, 1009, **1013**, **1022**, 1027, 1039, 1042, 1045, **1046**, 1054, 1057, **1070**, **1073**, 1078, **1085**, 1087, 1093, **1094**, **1106**, 1111, 1126, **1133**, **1145**, 1150, **1160**, **1166**, **1172**, 1178, **1184**, 1186, 1189, 1190, 1205, **1208**, 1213, **1217**, 1223, 1231, 1243, 1255, 1258, 1261, **1262**, **1271**, 1276, 1279, **1286**, **1295**, 1297, 1303, **1310**, **1316**, 1318, 1330, 1342, **1346**, 1354, **1358**, 1366, **1367**, **1373**, **1388**, 1390, **1400**, 1405, 1406, 1418, **1424**, 1426, **1439**, **1442**, 1445, 1453, **1457**
$GF(2187)$	312	156	2198, **2203**, **2206**, 2213, **2218**, 2219, 2225, **2227**, **2233**, 2237, 2255, 2258, **2263**, 2266, 2285, 2294, 2297, **2305**, **2317**, **2323**, 2330, **2335**, 2342, **2365**, **2374**, **2377**, 2390, 2396, 2405, **2410**, **2413**, 2426, **2434**, 2435, 2441, 2447, **2449**, **2455**, **2467**, 2471, 2477, **2479**, 2495, **2503**, 2519, **2521**, **2533**, **2539**, 2549, **2554**, **2557**, 2567, 2570, **2572**, **2578**, 2582, **2599**, 2606, 2612, 2621, 2630, **2638**, 2645, **2647**, **2650**, 2654, 2669, **2671**, **2674**, 2675, **2683**, 2687, 2693, **2695**, **2707**, 2708, **2716**, 2726, **2731**, 2732, **2755**, **2770**, 2774, **2791**, **2794**, 2798, **2806**, **2812**, 2816, **2818**, 2822, 2831, 2837, **2845**, 2861, 2879, 2882, 2885, **2887**, 2894, **2896**, **2902**, 2909, **2911**, **2926**, 2942, 2951, 2957, **2965**, 2975, 2978, **2986**, 2990, **2998**, 3005, **3013**, **3022**, **3037**, 3044, 3053, 3062, 3074, **3085**, 3086, 3089, 3092, **3097**, 3104, **3118**, 3122, **3124**, 3128, **3142**, 3149, **3154**, **3157**, 3161, 3167, **3175**, 3182, 3191, 3194, 3197, **3199**, **3202**, 3215, **3226**, 3239, **3241**, 3245, **3253**, 3254, **3262**, 3266, **3271**, **3274**, **3286**, 3293, **3298**, **3319**, 3332, **3334**, 3338, 3344, **3346**, **3349**, **3358**, 3368, **3382**, 3389, **3394**, 3401, **3421**, 3422, 3434, **3436**, **3439**, **3442**, **3454**, 3455, 3458, **3472**, **3478**, 3479, 3485, **3487**, **3490**, **3493**, **3511**, 3518, 3527, 3533, **3535**, 3542, 3551, 3557, **3565**, 3578, **3586**, 3599, 3602, 3605, **3607**, **3622**, 3629, 3635, **3637**, **3643**, **3661**, 3665, **3679**, 3686, **3694**, **3703**, **3706**, **3709**, 3725, **3733**, 3734, 3737, **3742**, **3745**, **3748**, 3764, **3766**, 3776, **3778**, 3794, 3797, 3800, **3805**, 3809, **3814**, 3824, 3833, **3844**, 3857, **3862**, **3874**, **3880**, **3889**, **3895**, **3901**, 3914, **3919**, **3922**, **3934**, 3938, 3941, **3943**, **3958**, 3965, **3982**, 3986, **3988**, 3992, **3994**, 3998, **4006**, 4016, 4031, 4034, **4039**, **4045**, 4052, **4054**, 4064, **4066**, **4072**, 4073, 4082, 4085, 4088, **4093**, 4109, 4121, **4141**, 4142, **4162**, 4166, **4174**, 4175, 4178, 4181, **4186**, **4198**, 4199, 4211, 4214, 4226, **4234**, **4246**, **4258**, **4261**, 4265, 4271, 4277, 4283, **4285**, **4291**, **4294**, 4298, 4301, 4313, 4322, **4327**, **4333**, 4337, **4345**, **4351**, **4357**, **4369**

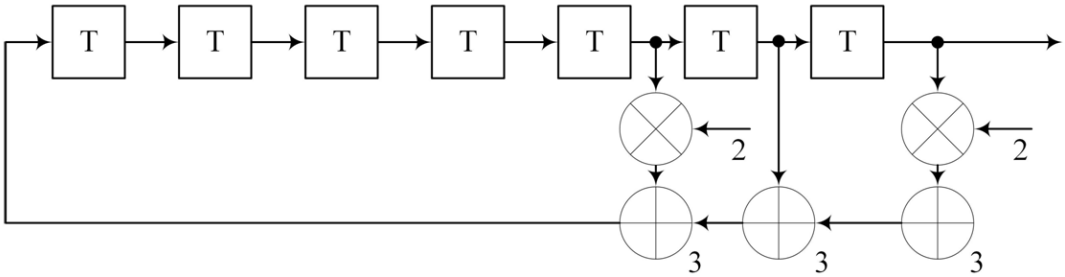

Рисунок 2.2 – 3РСЛОС на основе первообразного полинома $f_1(\rho) = \rho^7 + \rho^2 + 2\rho + 1$

а также выбраны первообразные полиномы (таблица 2.1), определяющие структуры соответствующих РСЛОС (f_{bin}) и 3РСЛОС (f_i)

$$\begin{cases} f_1(\rho) = 2203_{10} = \rho^7 + \rho^2 + 2\rho + 1; \\ f_2(\rho) = 734_{10} = \rho^6 + \rho + 2; \\ f_3(\rho) = 307_{10} = \rho^5 + 2\rho^3 + \rho^2 + 1; \\ f_{bin}(\rho) = \rho^{14} + 1, \end{cases}$$

и их исходные состояния

$$\beta_1 = \{1111111\}, \beta_2 = \{111111\}, \quad \beta_3 = \{11111\}, \beta_4 = \{11111111111111\}. \tag{2.1}$$

На основе каждого полинома может быть построена схема РСЛОС, как это показано в [6]. Начальные условия РСЛОС представляют собой элемент ключевой информации. Например, схема 3РСЛОС, основанная на полиноме

$$f_1(\rho) = \rho^7 + \rho^2 + 2\rho + 1,$$

приведена на рисунке 2.2.

Учитывая исходные состояние РСЛОС (2.1), генерируемые последовательности будут иметь следующий вид

$$\xi_1 = \{11111112222212111200\ldots\};$$
$$\xi_2 = \{11111100000100002100\ldots\};$$
$$\xi_3 = \{11111220200200102222\ldots\};$$
$$\xi_4 = \{11111111111111111000\ldots\}.$$

Рассмотрим процесс генерации первого трита ключевой последовательности. Основываясь на рисунке 2.1 бит последовательности ξ_4 определяет нам выбор тройственного набора, и поскольку он равен 1, то используется тройственный набор 1. Трит последовательности ξ_3 определяет выбор 3-бент-последовательности внутри тройственного набора, и поскольку, в нашем случае, он также равен 1, выбирается 3-бент-последовательность $БФ_5$. Триты последовательностей ξ_1 и ξ_2 являются аргументами 3-бент-функции или, соответственно, определяют конкретную координату таблицы истинности 3-бент-последовательности, которая подается на выход схемы. В нашем случае это $11_3 = 4$ координата (нумерация начинается с 0) 3-бент-последовательности и поэтому $\gamma = 1\ldots$. Повторяя подобные расчеты, вычисляем последующие элементы результирующей ключевой последовательности $\gamma = \{11111102022212112100\ldots\}$.

Результаты проведенного анализа стохастических характеристик [3] предложенного ГПКП для длины гаммы 3^{12} бит представлены в таблице 2.2, где знак «+» означает, что данный критерий выполняется, а знак «–» – не выполняется.

Таблица 2.2 – Стохастические характеристики предложенного ГПКП

№ п/п	Критерии качества	Предложенный ГПКП
1	Сбалансированность	177402/177114/176925
2	Случайный внешний вид сигнала	+
3	Равномерное распределение гистограммы	+
4	Случайное распределение на плоскости	+
5	2-х граммное распределение	+
6	3-х граммное распределение	+
7	4-х граммное распределение	+
8	Монотонность	+
9	Линейная сложность	+
10	Максимальный боковой лепесток битовой АКФ	0,0092
11	Спектральный тест	+
12	Стопка книг [14]	+

Анализ данных таблицы 2.2 показывает, что разработанный ГПКП соответствует базовым стохастическим тестам, предложенным в [3], а также тесту «Стопка книг» [14].

Определим число уровней защиты [15] разработанного ГПКП для нашего примера. Начальное значение $3РСЛОС_1$ может быть выбрано $3^7 - 1 = 2186$ способами, $3РСЛОС_2$ – $3^6 - 1 = 728$ способами, $3РСЛОС_3$ – $3^5 - 1 = 242$ способами, тогда как двоичного $РСЛОС_4$ – $2^{14} - 1 = 16383$ способами. Шесть 3-бент-последовательностей из полного множества могут быть выбраны $108^3 \cdot 54^3 \approx 1.07 \cdot 10^{13}$ способами. Таким образом,

число уровней защиты рассматриваемого в качестве примера ГПКП определяется как

$$\Psi = 1.07 \cdot 10^{13} \cdot 2186 \cdot 728 \cdot 242 \cdot 16383 \approx 6.75 \cdot 10^{25},$$

тогда как длина ключа равна $|K| = \lceil \log_2 \Psi \rceil = 86$ бит или $|K| = \lceil \log_3 \Psi \rceil = 55$ трит.

Число уровней защиты является легко масштабируемым за счет применения бóльших степеней полиномов для РСЛОС или бóльших длин 3-бент-последовательностей. Последнее, несомненно, требует детального изучения классов 3-бент-последовательностей бóльших длин, что может стать предметом дальнейших исследований.

Заключение

Отметим основные результаты проведенных исследований:

1. Разработан троичный ГПКП на основе тройственных наборов 3-бент-последовательностей, обладающий высоким уровнем стохастического и криптографического качества, который может быть использован как в современных *q*-ичных телекоммуникационных системах, так и в криптографических приложениях. В частности, перспективным и более практичным, в сравнении с двоичным, является применение троичного варианта рассмотренных конструкций в JPEG и MPEG.

2. Найден полный класс 3-бент-последовательностей и проведена его классификация на тройственные наборы по критерию различных весовых структур.

3. Дальнейшее развитие получил метод нахождения АНФ логических функций, в рамках чего разработан алгоритм нахождения АНФ 3-функций, который может быть использован при решении многих прикладных задач.

ЛИТЕРАТУРА

1. *Агафонова*, *И.В*. Криптографические свойства нелинейных булевых функций / И.В. Агафонова // Семинар по дискрет. гармон. анализу и геометр. моделированию. – СПб.: DHA & CAGD, 2007. – С. 1–24.

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. – Вып. 3 (42). – С. 150–156.

3. *Иванов*, *М.А*. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

4. *Соколов*, *А.В*. Быстродействующий генератор ключевых последовательностей на сонове клеточных автоматов / А.В. Соколов. – Одесса: Труды ОНПУ, 2014. – № 1 (43). – С. 180 –186.

5. *Рябко*, *Б.Я*. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. – М.: Горячая линия – Телеком, 2010. – 232 с.

6. *Мазурков*, *М.И*. Системы широкополосной радиосвязи / М.И. Мазурков // Одесса: Наука и Техника, 2010. – 340 с.

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

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

9. *Meng Qing-shu*. A novel algorithm enumerating bent functions / Meng Qing-shu, Yang min Cui jing-song // Discrete Mathematics. – 2008. – Vol. 308, Issue 23. – P. 5576–5584.

10. *Амбросимов*, *А.С*. Свойства бент-функций *q*-значной логики над конечными полями / А.С. Амбросимов // Дискретная математика. – 1994. – Т. 6, вып. 3. – С. 50–60.

11. *Kumar*, *P.V*. Generalized bent functions and their properties / P.V. Kumar, R.A. Scholtz, L.R. Welch // J. Combin. – Theory Ser A. – 1985. – № 40 (1). – P. 90–107.

12. *Соколов*, *А.В*. Построение троичных бент-последовательностей / А.В. Соколов, О.Н. Жданов, Н.А. Барабанов // Материалы XIX международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», Харьков. – 2015. – Т. 3. – С.131–132.

13. *Питерсон*, *У*. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон. – М.: Мир, 1976. – 598 с.

14. *Рябко*, *Б.Я*. «Стопка книг» как новый статистический тест для случайных чисел / Б.Я. Рябко, А.И. Пестунов. – Проблемы передачи информации. – 2004. – № 40:1. – С. 73–78.

15. *Мазурков*, *М.И*. Трехуровневая криптографическая система блочного шифрования данных / М.И. Мазурков, В.Я. Чечельницкий, К. Некрасов // Известия высших учебных заведений. Радиоэлектроника. – 2010. – Т. 53, № 7. – С. 43–47.

Поступила в редакцию 15.12.15.