УДК 681.3.06

**МАЗУРКОВ М.И., СОКОЛОВ А.В., БАРАБАНОВ Н.А.**

# МЕТОД СИНТЕЗА БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ В БАЗИСЕ ВИЛЕНКИНА-КРЕСТЕНСОНА

*Одесский национальный политехнический университет,*
*Украина, Одесса, 65044, пр. Шевченко, 1*

**Аннотация**. В статье разработан метод построения полного класса бент-последовательностей длины $N = 9$ в базисе Виленкина-Крестенсона, основанный на применении трех опорных конструкций. Первая конструкция допускает построение бент-последовательностей произвольной длины $N = 3^{2k}, k \in \mathbb{N}$. Полученные бент-последовательности могут быть использованы как в приложениях криптографии, так и в качестве кодов постоянной амплитуды в технологии MC-CDMA. Предложена также конструкция блока гаммирования графической и видео информации на основе бент-последовательностей в базисе Виленкина-Крестенсона.

**Ключевые слова**: бент-последовательность, преобразование Виленкина-Крестенсона, регулярный метод.

**Abstract.** In this paper we developed a synthesis method of complete class of bent-sequences of length $N = 9$ in the Vilenkin-Christenson basis, based on the use of three bearing formations. The first formation allows to construct a bent-sequences of any length $N = 3^{2k}, k \in \mathbb{N}$. Obtained bent-sequences can be used in applications of cryptography and constant-amplitude codes design for MC-CDMA technology. We also propose a gamma block design based on bent-sequences in the Vilenkin-Christenson basis for graphic and video information encryption.

**Keywords**: bent-sequence, Vilenkin-Christenson transform, a regular method.

В последние десятилетия совершенные алгебраические конструкции получили свои множественные применения в различных приложениях теории радиосвязи, передачи информации, а также криптографии [1]. Одними из наиболее применяемых совершенных алгебраических конструкций в области криптографии являются бент-последовательности, представляющие собой таблицы истинности бент-функций — наиболее нелинейных булевых функций, обладающих равномерным спектром Уолша-Адамара.

В литературе известны эффективные и быстродействующие генераторы псевдослучайных ключевых последовательностей (ГПКП) на основе дуальных пар бент-функций [2, 3], которые могут быть положены в основу алгоритмов поточного шифрования, блоков гаммирования блочных алгоритмов шифрования, а также применены для генерации ключевой информации.

Развитие принципов многозначной логики, в частности, разработка методов построения многозначных совершенных алгебраических конструкций является необходимой для повышения эффективности систем шифрования и скремблирования графической и видео информации. Многие современные системы обработки графической информации основаны на принципе разделения потока данных на цветовые составляющие в соответствии с цветовой моделью. Чаще всего применяются цветовые модели, такие как RGB, основанные на представлении цветов в виде кортежей трех чисел, называемых цветовыми компонентами. Так при выполнении операции гаммирования, данные кортежи объединяются в одно число, которое и складывается с гаммой. Таким образом, необходимая длина ключевой последовательности должна быть в 3 раза больше чем длина ключевой последовательности, необходимой для шифрования изображения такого-же размера, но заданного в градациях серого цвета. Данное обстоятельство является нежелательным при шифровании/скремблировании большого количества изображений в реальном масштабе времени, например, для передачи по сети.

Использование таких совершенных алгебраических конструкций как многозначные бент-функции [4] позволяет построить системы, допускающие одновременную обработку всех трех цветовых компонент.

Бент-функции также находят свои множественные применения в технологии кодового разделения каналов MC-CDMA для построения кодов постоянной амплитуды, обладающих оптимальным значением пик-фактора $\kappa = 1$ [5]. Применение подобных кодов позволяет существенно повысить эффективность использования мощности передатчика, а также снизить уровень нелинейных искажений.

Одно из перспективных направлений развития технологии MC-CDMA сопряжено с внедрением принципов многозначной логики путем перехода к использованию преобразования Виленкина-Крестенсона [6]. Данный подход требует проведения дальнейших исследований, направленных на построение новых многозначных кодов постоянной амплитуды, основанных на бент-последовательностях в базисе Виленкина-Крестенсона.

Еще одним практически важным применением многозначных совершенных алгебраических конструкций является квантовая криптография, для задач которой требуется построение генераторов многозначных псевдослучайных последовательностей, обладающих высоким уровнем стохастического и криптографического качества [7].

Как показывают проведенные исследования, многозначные бент-последовательности являются качественным базисом для решения рассмотренных прикладных задач.

*Целью данной статьи является разработка метода синтеза бент-последовательностей в базисе Виленкина-Крестенсона длины* $N = 9$.

**Определение 1.** 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.

Функция трехзначной логики (3-функция) — это отображение $\{0,1,2\}^k \to \{0,1,2\}$, т.е. правило, однозначно сопоставляющее вектору из $k$ координат, принимающих значения 0,1,2 значение 0,1 или 2.

**Определение 2**. *Линейной* называется $q$-функция, аналитически задаваемая как

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

где $a_0, a_1, ..., a_{k-1} \in \{0,1,...,q-1\}$.

Для случая $k = 2$, существует 3 линейные функции, задаваемые как $\varphi'(x_0) = \mathrm{a}_0\, x_0 \bmod 3$, для $a_0, x_0 \in \{0,1,2\}$

$$f_1 = [000], \quad f_2 = [012], \quad f_3 = [021]. \qquad (2)$$

На основе полученных линейных функций, а также однозначного преобразования $0 \to e^{j0^\circ}, 1 \to e^{j120^\circ}, 2 \to e^{j240^\circ} = e^{-j120^\circ}$, которое устанавливает взаимосвязь между символической и экспоненциальной формой представления 3-функций запишем матрицу преобразования Виленкина-Крестенсона

$$V_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \to \begin{bmatrix} e^{j0} & e^{j0} & e^{j0} \\ e^{j0} & e^{j120} & e^{j240} \\ e^{j0} & e^{j240} & e^{j120} \end{bmatrix}, \qquad (3)$$

которая является ортогональной, т.е. $V_3 V_3^T = 3E$, где $E$ — единичная матрица.

С другой стороны, по определению [8] ортогональные функции, определяющие строки матрицы преобразования Виленкина-Крестенсона могут быть заданы как

$$v_t(x) = \mathrm{e}^{\frac{2\pi}{q}\sum_{i=1}^{k} t_i x_i}, \tag{4}$$

где $q$ — основание системы счисления;

$t_i$ — $i$-й разряд числа $t$ записанного в позиционной $q$-ичной системе;

$k$ — число разрядов в $q$-ичном представлении значения $N$, которое определяет длину выборочных отсчетов сигнала, причем $N = q^k$.

Спектр дискретной последовательности находится путём умножения вектора-столбца, содержащего отсчёты сигнала, на комплексно сопряженную матрицу преобразования $\overline{V}$.

Проведенные исследования позволили найти упрощенное правило рекуррентного построения матриц Виленкина-Крестенсона любого порядка $\mu = 3^L$, $L \in \mathbb{N}$

$$V_{3^L} = \begin{bmatrix} V_{3^{L-1}} & V_{3^{L-1}} & V_{3^{L-1}} \\ V_{3^{L-1}} & \left(V_{3^{L-1}} + 1\right) \bmod 3 & \left(V_{3^{L-1}} + 2\right) \bmod 3 \\ V_{3^{L-1}} & \left(V_{3^{L-1}} + 2\right) \bmod 3 & \left(V_{3^{L-1}} + 1\right) \bmod 3 \end{bmatrix}. \tag{5}$$

В работе [9] введено определение бент-последовательности в базисе Виленкина-Крестенсона, и установлено, что для длины $N = 9$, существует множество из $J = 486$ бент-последовательностей.

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

$$\Omega_B(\omega) = \left| H \cdot \overline{V}_N \right| = const, \quad \omega = \overline{0, N-1}, \tag{6}$$

где $V_N$ — матрица Виленкина-Крестенсона порядка $N$.

В настоящей статье предлагается регулярный метод построения бент-последовательностей в базисе Виленкина-Крестенсона, основанный на трех конструкциях, для каждой из которых найдены правила размножения.

*Конструкция 1.*

Для построения бент-последовательности в базисе Виленкина-Крестенсона длины $N = 9$ проведем последовательную конкатенацию строк матрицы (3)

$$B = [000012021] = \left[ e^{j0} \quad e^{j0} \quad e^{j0} \quad e^{j0} \quad e^{j120} \quad e^{j240} \quad e^{j0} \quad e^{j240} \quad e^{j120} \right]. \tag{7}$$

Для того, чтобы убедиться, что построенная последовательность действительно представляет собой бент-последовательность проведем её умножение на матрицу Виленкина-Крестенсона порядка 9, построенную в соответствии с (5)

$$V_9 = \begin{bmatrix} e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} \\ e^{j0^o} & e^{j120^o} & e^{j240^o} & e^{j0^o} & e^{j120^o} & e^{j240^o} & e^{j0^o} & e^{j120^o} & e^{j240^o} \\ e^{j0^o} & e^{j240^o} & e^{j120^o} & e^{j0^o} & e^{j240^o} & e^{j120^o} & e^{j0^o} & e^{j240^o} & e^{j120^o} \\ e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j120^o} & e^{j120^o} & e^{j120^o} & e^{j240^o} & e^{j240^o} & e^{j240^o} \\ e^{j0^o} & e^{j120^o} & e^{j240^o} & e^{j120^o} & e^{j240^o} & e^{j0^o} & e^{j240^o} & e^{j0^o} & e^{j120^o} \\ e^{j0^o} & e^{j240^o} & e^{j120^o} & e^{j120^o} & e^{j0^o} & e^{j240^o} & e^{j240^o} & e^{j120^o} & e^{j0^o} \\ e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j240^o} & e^{j240^o} & e^{j240^o} & e^{j120^o} & e^{j120^o} & e^{j120^o} \\ e^{j0^o} & e^{j120^o} & e^{j240^o} & e^{j240^o} & e^{j0^o} & e^{j120^o} & e^{j120^o} & e^{j240^o} & e^{j0^o} \\ e^{j0^o} & e^{j240^o} & e^{j120^o} & e^{j240^o} & e^{j120^o} & e^{j0^o} & e^{j120^o} & e^{j0^o} & e^{j240^o} \end{bmatrix}. \quad (8)$$

В результате чего получаем спектр последовательности (7)

$$S = \left[ 3 \cdot e^{j0} \quad 3 \cdot e^{j0} \quad 3 \cdot e^{j0} \quad 3 \cdot e^{j0} \quad 3 \cdot e^{-j120} \quad 3 \cdot e^{j120} \quad 3 \cdot e^{j0} \quad 3 \cdot e^{j120} \quad 3 \cdot e^{-j120} \right]. \quad (9)$$

То есть последовательность (7) действительно соответствует *Определению 3* и является бент-последовательностью в базисе Виленкина-Крестенсона.

Приведем правила размножения:

*Правило 1.* При конкатенации строк матрицы Виленкина-Крестенсона их перестановка может быть выполнена $\mu! = 3^L !$ способами.

Для нашего примера (3) строки матрицы Виленкина-Крестенсона порядка $\mu = 3$ могут быть переставлены $3! = 6$ способами, в результате чего получаем 6 новых бент-последовательностей в базисе Виленкина-Крестенсона

$$\begin{bmatrix} \{0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1\} \\ \{0 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 2\} \\ \{0 & 1 & 2 & 0 & 0 & 0 & 0 & 2 & 1\} \\ \{0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0\} \\ \{0 & 2 & 1 & 0 & 1 & 2 & 0 & 0 & 0\} \\ \{0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 & 2\} \end{bmatrix}. \quad (10)$$

*Правило 2.* Относительно каждой строки матрицы Виленкина-Крестенсона может быть применена операция перекодирования всеми возможными правилами путем прибавления числа 0, 1 или 2 по $\mathrm{mod}\, 3$.

Для нашего примера $\mu = 3$ (3) каждая строка может быть закодирована тремя способами, таким образом мощность *Правила 2* составляет $J = 27$ последовательностей на основе одной.

$$\begin{bmatrix} \{000012021\} & \{111012021\} & \{222012021\} \\ \{000012102\} & \{111012102\} & \{222012102\} \\ \{000012210\} & \{111012210\} & \{222012210\} \\ \{000120021\} & \{111120021\} & \{222120021\} \\ \{000120102\} & \{111120102\} & \{222120102\} \\ \{000120210\} & \{111120210\} & \{222120210\} \\ \{000201021\} & \{111201021\} & \{222201021\} \\ \{000201102\} & \{111201102\} & \{222201102\} \\ \{000201210\} & \{111201210\} & \{222201210\} \end{bmatrix} \quad (11)$$

Комбинируя *Правило 1* и *Правило 2*, получаем первый класс бент-последовательностей в базисе Виленкина-Крестенсона мощности $J_1 = 6 \cdot 27 = 162$. Данный

класс является аналогом класса Майорана-МакФарланда [10] для двоичных бент-последовательностей.

Отметим, что использование данной конструкции и правил размножения для любого порядка матрицы Виленкина-Крестенсона определяет возможность построения бент-последовательностей в базисе Виленкина-Крестенсона любой длины $N = 3^{2k}$.

Так, например, на основе матрицы Виленкина-Крестенсона порядка $\mu = 3^2 = 9$ (8) могут быть построены бент-последовательности в базисе Виленкина-Крестенсона длины $N = 81$. Причем, с учетом правил размножения их количество будет определяться как $J_{1,81} = \mu! 3^{\mu} = 9! \cdot 3^9 = 7142567040$.

*Конструкция 2.*

Установлено, что синтез бент-последовательностей в базисе Виленкина-Крестенсона может быть произведен на основе следующих двух регулярных конструкций:

$$C_1 = \begin{bmatrix} r \\ r \\ (r+1) \bmod 3 \end{bmatrix}, \quad C_2 = \begin{bmatrix} r \\ r \\ (r+2) \bmod 3 \end{bmatrix}, \tag{12}$$

где $r$ — любая троичная последовательность, за исключением строк матрицы Виленкина-Крестенсона и их линейных комбинаций. Таким образом, в качестве $r$ могут быть использованы $27 - 9 = 18$ строк

$$\begin{bmatrix} \{001\} & \{100\} & \{200\} \\ \{002\} & \{101\} & \{202\} \\ \{010\} & \{110\} & \{211\} \\ \{011\} & \{112\} & \{212\} \\ \{020\} & \{121\} & \{220\} \\ \{022\} & \{122\} & \{221\} \end{bmatrix} \tag{13}$$

Очевидно, что последнюю строку конструкции мы можем переставить тремя различными способами, например, для первой конструкции

$$C_1 = \begin{bmatrix} r \\ r \\ (r+1) \bmod 3 \end{bmatrix}, \quad C_1' = \begin{bmatrix} r \\ (r+1) \bmod 3 \\ r \end{bmatrix}, \quad C_1'' = \begin{bmatrix} (r+1) \bmod 3 \\ r \\ r \end{bmatrix} \tag{14}$$

Таким образом, мощность класса составляет $J_2 = 3 \cdot 2\left(3^3 - 3^2\right) = 6\left(27 - 9\right) = 108$

*Конструкция 3.*

Еще одна конструкция, позволяющая синтез бент-последовательностей в базисе Виленкина-Крестенсона может быть записана как

$$C_1 = \begin{bmatrix} r \\ r \leftarrow 1 \\ (r+1) \bmod 3 \leftarrow 2 \end{bmatrix}, \quad C_2 = \begin{bmatrix} r \\ r \leftarrow 1 \\ (r+2) \bmod 3 \leftarrow 2 \end{bmatrix} \tag{15}$$

где оператор $\leftarrow$ обозначает циклический сдвиг влево на соответствующее число позиций;

$r$ — любая троичная последовательность, за исключением строк матрицы Виленкина-Крестенсона и их линейных комбинаций.

*Конструкция 3* может быть подвергнута всем возможным $3! = 6$ перестановкам. Таким образом, общая мощность третьего класса бент-последовательностей в базисе Виленкина-Крестенсона составляет $J_3 = 2 \cdot 6 \cdot \left(3^3 - 3^2\right) = 216$.

Объединяя все три класса бент-последовательностей в базисе Виленкина-Крестенсона, получаем полный класс мощности $J = 162 + 108 + 216 = 486$. Аналогичный результат может быть получен методом полного перебора.

Исследования, проведенные в [9] позволили классифицировать полное множество бент-последовательностей в базисе Виленкина-Крестенсона в зависимости от их весовой структуры на 6 классов

$$\begin{bmatrix} \{1,4,4\}(54); \\ \{4,1,4\}(54); \\ \{4,4,1\}(54); \end{bmatrix} \begin{bmatrix} \{5,2,2\}(108); \\ \{2,5,2\}(108); \\ \{2,2,5\}(108), \end{bmatrix} \tag{16}$$

где числа в фигурных скобках показывают, соответственно, количество символов «0», «1» и «2» в бент-последовательности, а числа в круглых скобках — количество бент-последовательностей, обладающих указанной структурой.

Таким образом, бент-последовательности из (16) определяют два тройственных набора

$$\begin{bmatrix} \{\{1,4,4\},\{4,1,4\},\{4,4,1\}\}, \\ \{\{5,2,2\},\{2,5,2\},\{2,2,5\}\}. \end{bmatrix} \tag{17}$$

**Определение 4.** Набор из трех бент-последовательностей $B_1, B_2, B_3$ в базисе Виленкина-Крестенсона называется тройственным набором, если конкатенация их таблиц истинности в символической форме является сбалансированной, т.е. количество символов «0» равно количеству символов «1» и равно количеству символов «2» $K^0 = K^1 = K^2$.

Установлено, что тройственные наборы бент-последовательностей в базисе Виленкина-Крестенсона могут использоваться как основа для построения блоков гаммирования изображений или потока видео, для чего может применяться схема, изображенная на рис. 1.

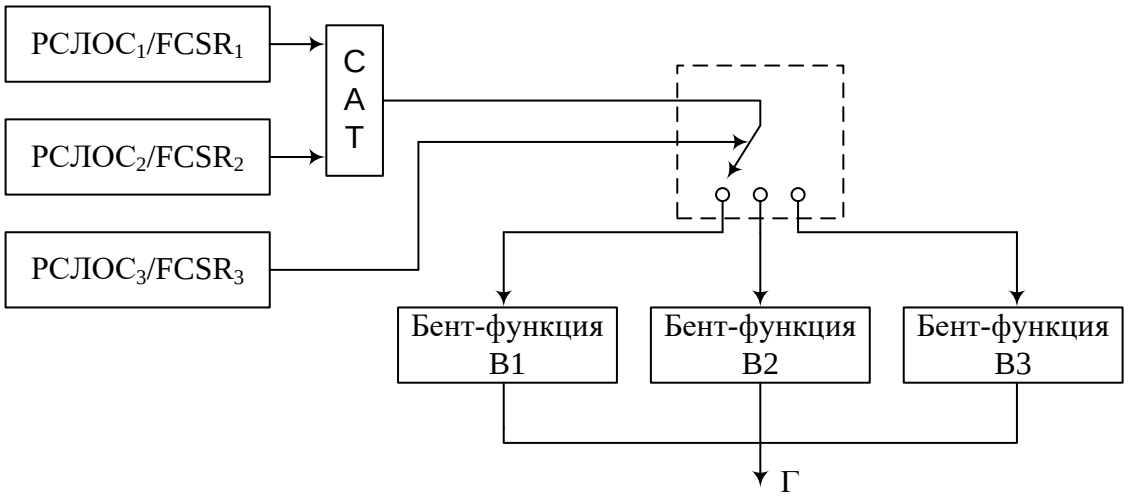


Рис. 1 — Генератор ключевой последовательности

На рис. 1 используются три троичных регистра сдвига с линейной обратной связью (РСЛОС) [1] или три троичных регистра сдвига с обратной связью по переносу (FCSR) [11] для генерации псевдослучайных последовательностей. Причем первые два регистра $\text{РСЛОС}_1/\text{FCSR}_1$ и $\text{РСЛОС}_2/\text{FCSR}_2$ используются для генерации аргумента бент-функции или номера координаты таблицы истинности бент-последовательности в базисе

Виленкина-Крестенсона, CAT — блок конкатенации. В это время регистр $\text{РСЛОС}_3/\text{FCSR}_3$, подключен к блоку выбора одной из трех бент-последовательностей $B_1$, $B_2$, $B_3$ представляющих собой тройственный набор.

Алгоритм применения результирующей последовательности $\Gamma$ к потоку изображения или видеопотоку, представленному цветовой моделью RGB:

1. Если $i$-й элемент ключевой последовательности равен нулю $\Gamma_i = 0$, то инвертируется соответствующий $i$-й бит канала $R$.

2. Если $i$-й элемент ключевой последовательности равен единице $\Gamma_i = 1$, то инвертируется соответствующий $i$-й бит канала $G$.

3. Если $i$-й элемент ключевой последовательности равен двойке $\Gamma_i = 2$, то инвертируется соответствующий $i$-й бит канала $B$.

Таким образом, за один такт работы генератора ключевой последовательности производится гаммирование одновременно всех цветовых потоков изображения или видео.

Рассмотрим пример работы генератора ключевых последовательностей (рис. 1). Пусть, например, выбрана схема, содержащая регистры сдвига с обратной связью по переносу (FCSR) в общем виде представленная на рис.2.

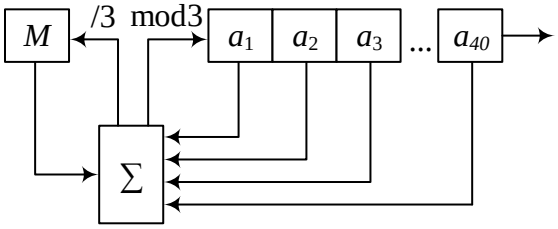


Рис. 2 — Регистр сдвига с обратной связью по переносу

В качестве исходных состояний $A = \{a_1, a_2, ..., a_{40}\}$ регистров FCSR выбраны следующие последовательности, которые являются ключом

$$\begin{aligned} A_1 &= \{0110100110212212002221100220201020220201\}; \\ A_2 &= \{2221221011020212112122122222021102120122\}; \\ A_3 &= \{0202010100111101121221002220111121200222\}, \end{aligned} \tag{18}$$

а ячейка переноса $M = 0$. Также выбран следующий тройственный набор бент-последовательностей в базисе Виленкина-Крестенсона

$$\begin{cases} B_1 = [102120222]; \\ B_2 = [121112100]; \\ B_3 = [102000201]. \end{cases} \tag{19}$$

Используя данные параметры несложно произвести генерацию ключевой последовательности $\Gamma$, после чего применить её к изображению/видео в соответствии с изложенным алгоритмом.

Исследования стохастических свойств многозначных псевдослучайных последовательностей, генерируемых схемой (рис. 1) с помощью набора тестов [7] показывает их полное соответствие критериям случайности.

Ясно, что один только блок гаммирования обеспечивает невысокую криптостойкость, однако, может применяться в приложениях требующих высокого

быстродействия. Тем не менее, разработанный блок гаммирвоания может быть использован как часть более сложных криптоалгоритмов, адаптированных к задачам шифрования изображений или видео.

Так, несложно оценить число уровней защиты разработанного генератора ключевых последовательностей (рис. 1) для приведенного примера. Очевидно, число исходных состояний трех регистров может быть задано приблизительно как $\sim 3^{120}$, тогда как наборы бент-последовательностей в базисе Виленкина-Крестенсона выбраны из первого тройственного набора (16) $54^3$ способами, либо же из второго $108^3$. Таким образом, общее число возможных выборов определятся как $54^3 + 108^3 = 1417176$. Общее число уровней защиты определяется как

$$\Psi \approx 3^{120} \cdot 1417176 \approx 2.546 \cdot 10^{63}, \tag{20}$$

и может быть легко масштабировано в соответствии с решаемыми задачами.

Вместо FCSR в схеме генератора (рис.1) могут быть применены обычные троичные РСЛОС, основанные на троичных первообразных полиномах.

Отметим также, что в предложенной схеме генератора ключевых последовательностей (рис. 1) могут использоваться бент-последовательности в базисе Виленкина-Крестенсона произвольной длины $N = 3^{2k}$, например, $N = 81$, построенные с помощью *Конструкции 1* и представляющие собой тройственный набор с величинами разбаланса $[K^0, K^1, K^2] = [33, 24, 24], [24, 33, 24], [24, 24, 33]$, соответственно, для каждой бент-последовательности в базисе Виленкина-Крестенсона

$$\begin{cases} B_1 = [000000000012012012021021021000111222012120201021102210000222111012201120021210102]; \\ B_2 = [111111111201201201021021021112220001202010121022100211100022210202121012001220 1]; \\ B_3 = [222222222012012012102102102220001112010121202100211022011200122221110002101020 21]. \end{cases} \tag{21}$$

В случае применения бент-последовательностей в базисе Виленкина-Крестенсона длины $N = 81$ в схеме генератора должны быть установлены пять РСЛОС или FCSR. Причем, $\text{РСЛОС}_1/\text{FCSR}_1$, $\text{РСЛОС}_2/\text{FCSR}_2$, $\text{РСЛОС}_3/\text{FCSR}_3$ и $\text{РСЛОС}_4/\text{FCSR}_4$ для генерации аргумента бент-функции или номера координаты таблицы истинности бент-последовательности в базисе Виленкина-Крестенсона, а регистр $\text{РСЛОС}_5/\text{FCSR}_5$ предназначен для выбора одной из трех бент-последовательностей $B_1$, $B_2$, $B_3$ (21).

Проведенные эксперименты позволили установить, что использование бент-последовательностей в базисе Виленкина-Крестенсона длины $N = 81$ также позволяет добиться полного сокрытия графической информации.

ВЫВОДЫ

1. В статье разработан регулярный метод синтеза полного класса бент-последовательностей длины $N = 9$ в базисе Виленкина-Крестенсона на основе трех опорных конструкций. При этом первая конструкция может быть использована для синтеза бент-последовательностей в базисе Виленкина-Крестенсона любой длины $N = 3^{2k}, k \in \mathbb{N}$. Синтезированные бент-последовательности применимы как для решения задач криптографии, так и для построения кодов постоянной амплитуды для технологии MC-CDMA.

2. На основе бент-последовательностей в базисе Виленкина-Крестенсона предложена схема блока гаммирования, которая может быть использована для обработки графической и видео информации.

3. Предложено быстрое рекуррентное правило построения матриц Виленкина-Крестенсона над алфавитом $e^{j0^{o}}, e^{j120^{o}}, e^{-j120^{o}}$ произвольного порядка $\mu = 3^{k}$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков // Одесса:Наука и Техника. — 2010. — с. 340. — ISBN 978-966-8335-95-2.
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. Соколов, А.В. Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов / А.В. Соколов. — Одесса: Труды ОНПУ, 2014 — №1(43). — С. 180 —186.
4. Амбросимов, А.С. Свойства бент-функций q-значной логики над конечными полями / А.С. Амбросимов // Дискрет. матем., 1994. — Т.6. — вып. 3. — С. 50—60.
5. Paterson K. G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic coding theory // K.G. Paterson. — Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. — P. 46–71.
6. Мазурков, М.И. О влиянии вида ортогонального преобразования на пик-фактор спектра сигналов в системах с CDMA / М.И. Мазурков, А.В. Соколов, Н.А. Барабанов // Информатика и математические методы в моделировании, 2015. — Т.5, №1. — С. 28—37.
7. Гнатюк, С.О. Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань / С.О. Гнатюк, Т.О. Жмурко, В.М. Кінзерявий, Н.А. Сєйлова // Information Technology and Security. – 2015. – Vol. 3. – № 2(5). – С. 108-116.
8. Трахтман, А.М. Основы теории дискретных сигналов на конечных интервалах. / А.М. Трахтман, В.А. Трахтман. — М.: Сов.радио, 1975. — 208 с.
9. Соколов А.В. О существовании троичных бент-последовательностей // А.В. Соколов, О.Н. Жданов, Н.А. Барабанов. — 19-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. материалов форума. Т. 3. — Харьков: ХНУРЭ. 2015. — С. 131—132.
10. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. — Томск, 2009. — Сер. №1(3). — С. 15—37.
11. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — Триумф, 2013. — 816 с.