УДК 004.056.55

А.А. Кузнецов[1], Л.Т. Пархуць[2] , Г.С. Цымбал[3]

[1] *Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[2] *Национальный университет «Львовская политехника», Львов*
[3] *Украинская государственная академия железнодорожного транспорта, Харьков*

ПОСТРОЕНИЕ НЕЛИНЕЙНЫХ ЭЛАСТИЧНЫХ ФУНКЦИЙ С ИСПОЛЬЗОВАНИЕМ ДВОИЧНЫХ БЛОКОВЫХ КОДОВ

Рассматриваются методы построения нелинейных узлов замен симметричных криптографических алгоритмов, исследуются показатели и критерии их эффективности. Рассматривается метод построения нелинейных эластичных функций из двоичных линейных блочных кодов, анализируется перспективность данного метода для получения функций с улучшенными показателями стойкости. Исследуются свойства синтезируемых булевых функций по различным показателям стойкости. Оценивается достигаемая нелинейность и эластичность для функций, полученных из различных классов линейных блоковых кодов, проводятся сравнения с другими методами синтеза и верхними теоретическими границами для сбалансированных криптографических функций.

Ключевые слова: *криптографические функции, нелинейность, сбалансированность, эластичность, корелляционный иммунитет, нелинейный узел замен.*

Постановка проблемы в общем виде и анализ литературы

Быстрое развитие современных компьютерных технологий обуславливает повышение вероятностно-временных требований к перспективным средствам защиты информации [1, 2]. Применяемые механизмы обеспечения безопасности должны удовлетворять высоким требованиям конфиденциальности, целостности и доступности информации.

Традиционный подход к обеспечению конфиденциальности информации состоит в использовании криптографических механизмов, таких, например, как блочное и поточное шифрование [1 – 4]. Проведенный анализ показал, что требуемый уровень безопасности обеспечивается применением соответствующих нелинейных функций усложнения (нелинейных узлов, блоков замен) в схеме шифрования, синтез которых и составляет одну из важнейших задач современной теории защиты информации [1 – 3]. В работах [3, 5, 6] показано, что криптографические булевы функции, описывающие нелинейные узлы замен в схеме шифрования могут быть эффективно синтезированы с помощью алгебраических методов, основанных на использовании линейных блоковых кодов. Криптографические свойства таких блоков усложнения непосредственно определяются характеристиками применяемых кодов.

Целью данной работы является исследование методов синтеза криптографических узлов замен, основанных на использовании линейных блоковых кодов, оценка показателей стойкости синтезируемых блоков усложнения, обоснование выбора направления дальнейших исследований.

Основные критерии и показатели эффективности нелинейных криптографических функций

Нелинейные криптографические функции, отображающие n-битные блоки входных данных в m-битные выходные блоки, обозначим в виде: $F: F_2^n \to F_2^m$. Любая функция F может быть изучена с помощью ее координатных функций, которые задаются в терминах булевой алгебры [3, 5, 6].

Рассмотрим криптографические свойства функций отображения из F_2^n в F_2^m, где $1 < m < n$. Пусть M_n^m есть множество таких функций. А B_n есть множество булевых функций от n переменных, то есть функций из F_2^n в F_2. Тогда любую функцию $F \in M_n^m$ можно рассматривать как состоящую из m булевых функций от n переменных, т.е. m-выходных координатных функции из B_n. В более общем представлении компонентная функция $F \in M_n^m$ является ненулевой линейной комбинацией ее координатных функций из B_n. Таким образом, функцию $F: F_2^n \to F_2^m$ запишем через множество

$$F = (f_1(x_1,...,x_n),...,f_m(x_1,...,x_n)),$$

где $f_i(x_1,...,x_n) \in B_n$.

Булева функция $f_i(x_1,...,x_n)$ может быть представлена в алгебраической нормальной форме (АНФ), то есть имеет уникальные двоичные константы $\lambda_0, \lambda_1,...,\lambda_{12},...,\lambda_{12...n}$ такие что:

$$f(x_1,...,x_n) = \lambda_0 + \lambda_1 x_1 + ... + \lambda_n x_n + \\ + \lambda_{12} x_1 x_2 + \lambda_{13} x_1 x_3 + ... + \lambda_{12...n} x_1 x_2 ... x_n, \quad (1)$$

где суммирование и умножение производится в двоичном поле F_2.

Определение 1 [3]. Алгебраическая степень f, обозначаемая $\deg(f)$, определяется как максимальная степень многочлена представленного в АНФ.

Важные свойства булевых функций изучается с использованием преобразования Уолша.

Определение 2 [3]. Преобразованием Уолша функции $f(x_1,...,x_n) \in B_n$ есть вещественная функция $\overline{F}(w)$:

$$\overline{F}(w) = \sum_{x \in F_2^n} (-1)^{f(x)+\omega \cdot x}, \quad (2)$$

где скалярное произведение векторов x и ω определяется как $x \cdot \omega = x_1\omega_1 + ... + x_n\omega_n$.

Булева функция f сбалансирована, если вероятности событий $f(x) = 1$ и $f(x) = 0$ равны. Используя преобразование Уолша, условие сбалансированности функции f запишем в виде $\overline{F}(0) = 0$.

Расстояние по Хеммингу между двумя функциями f и g из B_n определяется как:

$$d_H(f,g) = \text{card}\left\{ \begin{matrix} x \mid f(x) \neq g(x), \\ x \in F_2^n \end{matrix} \right\}. \quad (3)$$

Определение 3 [3]. Нелинейность $N(f)$ функции $f(x_1,...,x_n) \in B_n$ определяется как:

$$N(f) = \min_{g \in A_n} d_H(f,g), \quad (4)$$

где A_n это множество всех аффинных функций от n переменных,

$$A_n = \left\{ a_0 + \sum_{i=1}^{n} a_i x_i \mid a_i \in F_2, 0 \le i \le n \right\}.$$

С использованием преобразования Уолша нелинейность функции f может быть получена следующим образом:

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{w \in F_2^n} \left| \overline{F}(w) \right|. \quad (5)$$

Способность функций не пропускать информацию на выход для фиксированного подмножества входных переменных определяется эластичностью, которая в терминах преобразования Уолша была охарактеризована Ксао и Мэсси в [7].

Определение 4 [7]. Функция $f \in B_n$ эластична порядка t (t-эластична) тогда и только тогда, если:

$\overline{F}(w) = 0$ для всех $\omega \in F_2^n$ таких что

$$0 \le wt(\omega) \le t, \quad (6)$$

где $wt(\omega)$ определяется весом Хемминга ω, то есть, количеством единиц в ω.

Определение 5 [8]. Векторная булева функция $Y = F(X)(GF(2)^n \to GF(2)^m)$ называется (n,m,t) - эластичной, если любая частная функция, полученная из $F(X)$ фиксированием t переменных, является регулярной, т.е. ее значения пробегают все возможные m-граммы из $GF(2)^m$ равное количество раз в том случае, когда остальные $n-t$ переменных функции пробегают все 2^{n-t} значения из $GF(2)^{n-t}$ по одному разу. Параметр t называют эластичностью функции.

Следующая теорема устанавливает связь между эластичностью функции и ее компонентными функциями [3].

Теорема 1. Пусть t и m такие что $t+m \le n$. Функция $F = (f_1, f_2 ..., f_m)$ есть некая (n,m,t) – эластичная функция тогда и только тогда, когда все ненулевые комбинации $f_1,...,f_m$ являются $(n,1,t)$ - эластичными функциями, то есть t-эластичными функциями, принадлежащими B_n.

Определение 6 [3]. Нелинейность $N(F)$ функции $F = (f_1, f_2 ..., f_m)$ определяется как минимальная среди нелинейностей всех ее компонентных функций:

$$N(F) = \min_{b \in F_2^m, b \neq 0} N(f^{(b)}), \; f^{(b)} = \sum_{i=1}^{m} b_i f_i. \quad (7)$$

Аналогично, алгебраическая степень $F = (f_1, f_2 ..., f_m)$ определяется как минимальная степень компонентных функций F, а именно [1 – 3, 5 – 7]:

$$\deg(F) = \min_{b \in F_2^m, b \neq 0} \deg(f^{(b)}), \; f^{(b)} = \sum_{i=1}^{m} b_i f_i. \quad (8)$$

Предположим, что F является (n,m,t) - эластичной функцией, тогда справедлива граница [3]:

$$N(F) \le 2^{n-1} - 2^{t+1+\left\lfloor \frac{n-t-2}{r} \right\rfloor}, \quad (9)$$

где r получается из (8).

Эта граница справедлива для $n/2 - 2 \le t \le n/2$ и $n/2 \le m \le n/2 + 2$.

Эластичность t имеет также верхнюю границу [3]:

$$t \le \left\lfloor \frac{2^{m-1} n}{2^m - 1} \right\rfloor - 1. \quad (10)$$

Построение эластичных криптографических функций с высокими показателями нелинейности и алгебраической степени является важнейшей задачей в современной теории защиты информации.

В работах [3, 5 – 7] предложены методы синтеза эластичных функций, основанные на использовании двоичных блоковых кодов.

Построение эластичных функций на основе двоичных блоковых кодов

Связь между линейными эластичными функциями и линейными кодами была установлена в [9, 10]. Так любая граница характеристик линейных кодов приводит к некой границе по эластичности синтезируемых на их основе функций. Согласно предлагаемой конструкции, определяются линейные эластичные функции, функции координат которых и любая ненулевая линейная комбинация их линейны.

По определению, линейный блоковый двоичный код C длины n – это линейное подпространство в F_2^n, которое задается своей порождающей матрицей, строки которой формируют базис линейного кода C.

Минимальное кодовое расстояние есть наименьший вес Хемминга кодовых слов.

Соответственно, линейный двоичный код C длины n, размерностью m и минимальным кодовым расстоянием δ называют $[n, m, \delta]$ двоичным кодом.

Теорема 2 [11]. Пусть $C - [n, m, \delta]$ двоичный код, а G – его порождающая $m \times n$ матрица. Определим $F \in M_n^m$ следующим образом:

$$F(x_1, ..., x_n) = G \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Можно сказать, что F является (n, m, t)-эластичной функции. Такая функция F является линейной.

Другими словами, линейная (n, m, t)-эластичная функция существует тогда и только тогда, когда существует линейный $[n, m, t+1]$ код.

Как было показано в работе [12], используя любую нелинейную перестановку, линейную эластичную функцию легко можно превратить в нелинейную.

Теорема 3 [3, 12]. Пусть $H = P \circ F$, где F – линейная (n, m, t)-эластичная функция и пусть P – перестановка на F_2^m. Тогда имеем:

– некоторое m-мерное подпространство V на F_2^n, такое что ограничения H на V и на смежные классы V равны P;

– отображение H, $m \times 2^n$ матрица на F_2, может быть представлена как конкатенация из 2^{n-m} раз F_2^m, каждая часть является равной $P(V)$;

– степень H равна степени P;

– нелинейность H равна $2^{n-m} N(P)$.

Рассмотренная конструкция позволяет строить $(2^m - 1, m, 2^{m-1} - 1)$-эластичные функции H, нелинейность которых по крайней мере равна $2^{2^m-2} - 2^{2^m-1-(m/2)}$ и алгебраическая степень $m-1$.

Можно улучшить конструкцию из теоремы 3, используя все ненулевые слова линейного кода.

Лемма 1. [3]. Пусть $C - [u, m, \delta]$ двоичный код, с порождающей матрицей G. Пусть β – примитивный элемент поля F_{2^m}, который обеспечивает полиномиальный базис $(1, \beta, ..., \beta^{m-1})$ поля F_{2^m}. Определим линейное биективное отображение $\phi : F_{2^m} \mapsto C$ следующим образом:

$$ц(a_0 + a_1 в + ... + a_{m-1} в^{m-1}) = (a_0 ... a_{m-1})G$$

(просто кодируя $(a_0 ... a_{m-1})$). Получаем $2^m - 1 \times m$ матрицу:

$$A = \begin{pmatrix} ц(1) & ц(в) & \cdots & ц(в^{m-1}) \\ ц(в) & ц(в^2) & \cdots & ц(в^m) \\ \vdots & \vdots & \ddots & \vdots \\ ц(в^{2^m-2}) & ц(1) & \cdots & ц(в^{m-2}) \end{pmatrix}.$$

Тогда, для любой ненулевой линейной комбинации колонок матрицы A, каждое ненулевое кодовое слово C встретится только единожды. Мы можем получить (n, m, t)-эластичную функцию, нелинейность которой будет равна [3]:

$$N(F) = 2^{n-1} - 2^{u-1}. \qquad (11)$$

Приведенная лемма улучшает конструкцию из теоремы 3. Поясним это примером.

Пример. Пусть задан код $C - [7, 4, 3]$ двоичный линейный код Хэмминга с порождающей матрицей:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Используя терему 2, определим $(7, 4, 2)$ линейную эластичную функцию $F \in M_n^m$:

$$F(x_1 ... x_7) = \begin{cases} f_1 = x_1 + x_2 + x_4 \\ f_2 = x_2 + x_3 + x_5 \\ f_3 = x_3 + x_4 + x_6 \\ f_4 = x_4 + x_5 + x_7 \end{cases}.$$

Согласно Лемме 1, можно записать биективное отображение

$$\varphi : F_{2^m} \to C : \varphi(a_0 + a_1 \beta + . + {}_m {}^{m-1} a = /$$
$$= (a_0 + ... + a_m)G,$$

как:

$$\varphi(a_0 + a_1\beta + ... + a_m\beta^{m-1}) =$$

$$= \begin{bmatrix} a_0 & a_0 & 0 & a_0 & 0 & 0 & 0 \\ 0 & a_1 & a_1 & 0 & a_1 & 0 & 0 \\ 0 & 0 & a_2 & a_2 & 0 & a_2 & 0 \\ 0 & 0 & 0 & a_3 & a_3 & 0 & a_3 \end{bmatrix} =$$

$$= (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2 + a_3, a_1 + a_3, a_2, a_3).$$

Код (7,4,3) имеет 15 ненулевых кодовых слов, запишем матрицу в соответствии с Леммой 1:

$$A = \begin{vmatrix} \varphi(1) & \varphi(в) & \varphi(в^2) & \varphi(в^3) \\ \varphi(в) & \varphi(в^2) & \varphi(в^3) & \varphi(в^4) \\ \varphi(в^2) & \varphi(в^3) & \varphi(в^4) & \varphi(в^5) \\ \varphi(в^3) & \varphi(в^4) & \varphi(в^5) & \varphi(в^6) \\ \varphi(в^4) & \varphi(в^5) & \varphi(в^6) & \varphi(в^7) \\ \varphi(в^5) & \varphi(в^6) & \varphi(в^7) & \varphi(в^8) \\ \varphi(в^6) & \varphi(в^7) & \varphi(в^8) & \varphi(в^9) \\ \varphi(в^7) & \varphi(в^8) & \varphi(в^9) & \varphi(в^{10}) \\ \varphi(в^8) & \varphi(в^9) & \varphi(в^{10}) & \varphi(в^{11}) \\ \varphi(в^9) & \varphi(в^{10}) & \varphi(в^{11}) & \varphi(в^{12}) \\ \varphi(в^{10}) & \varphi(в^{11}) & \varphi(в^{12}) & \varphi(в^{13}) \\ \varphi(в^{11}) & \varphi(в^{12}) & \varphi(в^{13}) & \varphi(в^{14}) \\ \varphi(в^{12}) & \varphi(в^{13}) & \varphi(в^{14}) & \varphi(1) \\ \varphi(в^{13}) & \varphi(в^{14}) & \varphi(1) & \varphi(в) \\ \varphi(в^{14}) & \varphi(1) & \varphi(в) & \varphi(в^2) \end{vmatrix},$$

где $\varphi(\beta^i)$ – i -е кодовое слово.

Линейные компонентные функции будут иметь вид:

$$l_i(x) = \varphi(в^i) \cdot x$$
$$l_0(x) = (1101000) \cdot x = x_1 + x_2 + x_4$$
$$l_1(x) = (0110100) \cdot x = x_2 + x_3 + x_5$$
$$l_2(x) = (0011010) \cdot x = x_3 + x_4 + x_6$$
$$l_3(x) = (0001101) \cdot x = x_4 + x_5 + x_7$$
$$l_4(x) = (1011100) \cdot x = x_1 + x_3 + x_4 + x_5$$
$$l_5(x) = (1110010) \cdot x = x_1 + x_2 + x_3 + x_6$$
$$l_6(x) = (1000110) \cdot x = x_1 + x_5 + x_6$$
$$l_7(x) = (0101110) \cdot x = x_2 + x_4 + x_5 + x_6$$
$$l_8(x) = (1010001) \cdot x = x_1 + x_3 + x_7$$
$$l_9(x) = (0111001) \cdot x = x_2 + x_3 + x_4 + x_7$$
$$l_{10}(x) = (1100101) \cdot x = x_1 + x_2 + x_5 + x_7$$
$$l_{11}(x) = (0100011) \cdot x = x_2 + x_6 + x_7$$
$$l_{12}(x) = (1001011) \cdot x = x_1 + x_4 + x_6 + x_7$$
$$l_{13}(x) = (0010111) \cdot x = x_3 + x_5 + x_6 + x_7$$
$$l_{14}(x) = (1111111) \cdot x = x_1 + x_2 + x_3 + x_4 +$$
$$+ x_5 + x_6 + x_7.$$

Пусть будут добавлено две дополнительные переменные (y_1, y_2), тогда векторное пространство изменится с V_7 на V_9:

$$f_1 =$$
$$= (y_1 + 1)(y_2 + 1) \cdot l_0(x) + (y_1 + 1)y_2 \cdot l_1(x) +$$
$$+ y_1(y_2 + 1) \cdot l_2(x) + y_1y_2 \cdot l_3(x) = (y_1y_2 + y_1 +$$
$$+ y_2 + 1)l_0(x) + (y_1y_2 + y_2)l_1(x) +$$
$$+ (y_1y_2 + y_1)l_2(x) + y_1y_2l_3(x) = (y_1y_2 + y_1 +$$
$$+ y_2 + 1)(x_1 + x_2 + x_4) + (y_1y_2 + y_2)(x_2 +$$
$$+ x_3 + x_5) + (y_1y_2 + y_1)(x_3 + x_4 + x_6) +$$
$$+ y_1y_2(x_4 + x_5 + x_7)\Big|_{\substack{y_1 = x_8 \\ y_2 = x_9}} =$$
$$= (x_8x_9 + x_8 + x_9 + 1) \times$$
$$\times (x_1 + x_2 + x_4) + (x_8x_9 + x_9)(x_2 +$$
$$+ x_3 + x_5) + (x_8x_9 + x_8)(x_3 + x_4 + x_6) +$$
$$+ x_8x_9(x_4 + x_5 + x_7) = x_8x_9x_1 + x_8x_1 +$$
$$+ x_9x_1 + x_1 + x_8x_2 + x_2 + x_9x_4 + +x_4 +$$
$$+ x_9x_3 + x_9x_5 + .x_8x_3 + x_8x_9x_6 + x_8x_6 +$$
$$+ x_8x_9x_4 + x_8x_9x_7.$$

$$f_2 =$$
$$= (y_1 + 1)(y_2 + 1) \cdot l_1(x) + (y_1 + 1)y_2 \cdot l_2(x) +$$
$$+ y_1(y_2 + 1) \cdot l_3(x) + y_1y_2 \cdot l_4(x) = x_8x_9x_2 +$$
$$+ x_8x_2 + x_9x_2 + x_2 + x_8x_3 + x_3 + x_9x_5 + x_5 +$$
$$+ x_9x_4 + x_8x_9x_6 + .x_9x_6 + x_8x_4 + x_8x_9x_7 +$$
$$+ x_8x_7 + x_8x_9x_1 + x_8x_9x_3 + x_8x_9x_4 + x_8x_9x_5.$$

$$f_3 =$$
$$= (y_1 + 1)(y_2 + 1) \cdot l_2(x) + (y_1 + 1)y_2 \cdot l_3(x) +$$
$$+ y_1(y_2 + 1) \cdot l_4(x) + y_1y_2 \cdot l_5(x) = x_8x_6 + x_9x_3 +$$
$$+ x_9x_6 + x_8x_9x_7 + x_9x_5 + x_9x_7 + x_8x_9x_4 + .$$
$$+ x_8x_1 + x_8x_5 + x_8x_9x_2 + x_8x_9x_3 + x_3 + x_4 + x_6.$$

$$f_4 =$$
$$= (y_1 + 1)(y_2 + 1) \cdot l_3(x) + (y_1 + 1)y_2 \cdot l_4(x) +$$
$$+ y_1(y_2 + 1) \cdot l_5(x) + y_1y_2 \cdot l_6(x) = x_8x_9x_7 +$$
$$+ x_8x_4 + x_8x_5 + x_8x_7 + x_9x_7 + x_4 + x_5 + x_7 +$$
$$+ x_9x_1 + .x_9x_3 + x_8x_9x_2 + x_8x_1 + x_8x_2 +$$
$$+ x_8x_3 + x_8x_6 + x_8x_9x_1 + x_8x_9x_5.$$

В результате получена $(9,4,2)$ – нелинейная эластичная функция:

$$F(x)=\begin{cases} x_8x_9x_1+x_8x_1+x_9x_1+x_1+x_8x+x_2+ \\ +x_9x_4++x_4+x_9x_3+x_9x_5+x_8x_3+ \\ +x_8x_9x_6+x_8x_6+x_8x_9x_4+x_8x_9x_7, \\ \\ x_8x_9x_2+x_8x_2+x_9x_2+x_2+x_8x_3+x_3+ \\ +x_9x_5+x_5+x_9x_4+x_8x_9x_6+.x_9x_6+ \\ +x_8x_4+x_8x_9x_7+x_8x_7+x_8x_9x_1+ \\ +x_8x_9x_3+x_8x_9x_4+x_8x_9x_5, \\ \\ x_8x_6+x_9x_3+x_9x_6+x_8x_9x_7+x_9x_5+ \\ +x_9x_7+x_8x_9x_4+.x_8x_1+x_8x_5+ \\ +x_8x_9x_2+x_8x_9x_3+x_3+x_4+x_6, \\ \\ x_8x_9x_7+x_8x_4+x_8x_5+x_8x_7+x_9x_7+ \\ +x_4+x_5+x_7+x_9x_1+x_9x_3+x_8x_9x_2+ \\ +x_8x_1+x_8x_2+x_8x_3+x_8x_6+x_8x_9x_1+ \\ +x_8x_9x_5. \end{cases}$$

Нелинейность данной функции, согласно Лемме 1, $N(F)=2^{9-1}-2^{7-1}=192$, что легко проверить, используя формулу (5).

Таким образом, описанный метод позволяет формировать нелинейные эластичные функции с помощью линейных блоковых кодов. Суть метода заключается в использовании кодовых слов линейных блоковых кодов, которые посредством алгебраических преобразований с введением дополнительных переменных модифицируются до нелинейных эластичных функций с требуемыми параметрами.

В данной работе проводятся экспериментальные исследования свойств нелинейных узлов замен синтезированных рассмотренным методом для широкого класса линейных блоковых кодов, проводится также сравнение с верхней границей нелинейности и эластичности (1 – 3) и с наилучшими известными результатами формирования криптографических функций.

Результаты экспериментальных исследований

При проведении экспериментальных исследований были изучены нелинейные эластичные функции, полученные из следующих классов двоичных линейных блоковых кодов:

1. Код с проверкой на четность: $(n, n-1)$.

2. Код нечетной длины с повторением: $(n, 1, n)$.

3. Выколотый код Рида-Маллера 1-го порядка: $(2^p-1, p+1, 2^{p-1}-1)$.

4. Симплексный код: $(2^p-1, p, 2^{p-1})$.

5. Код Хэмминга: $(2^p-1, 2^p-p-1, 3)$.

6. Расширенный код Хэмминга: $(2^p, 2^p-p-1, 4)$.

7. Код БЧХ: $(2^p-1, 2^p-2p-1, 5)$.

8. Код Рида-Маллера первого порядка: $(2^p, p+1, 2^{p-1})$.

9. Укороченный код Хэмминга: $(2^p-1, 2^p-p-2, 4)$.

Как было показано выше, если существует $(u, m, t+1)$-линейный код, тогда можно построить $(u+k, m, t)$-нелинейную эластичную функцию [3, 5 – 7], где k – это количество дополнительных переменных, которые нужно добавить к линейной эластичной функции, образованной посредством алгебраической записи кодового слова линейного блокового кода, причем

$$u+k=n, \qquad (12)$$

где n – размерность векторного пространства (количество переменных синтезируемой функции).

Известно, что количество ненулевых слов линейного блокового кода $(u, m, t+1)$ равно [13]:

$$L_i=2^m-1. \qquad (13)$$

С другой стороны, для того, чтобы можно было добавить k переменных, понадобится L_i ненулевых кодовых слов, ограниченных снизу выражением:

$$L_i \geq 2^k+(m-1). \qquad (14)$$

Из (13) и (14) получаем формулу для расчета количества дополнительных переменных:

$$k \leq \lg_2(2^m-m). \qquad (15)$$

Таким образом, можем рассчитать, сколько может быть дополнительных переменных (k) при различных значениях информационных символов кода (m) (табл. 1).

Таблица 1

Зависимость количества дополнительных переменных от числа информационных символов кода

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
k ≤	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Из табл. 1 видно, что коды нечетной длины с повторением (№ 2) можно не рассматривать, так как, при $m=1$ количество дополнительных переменных $k=0$, а, следовательно, функции, построенные из этих кодов, являются линейными.

В табл. 2 представлены полученные результаты. В таблице приведены: столбец 1 – размерность векторного пространства; столбец 2 – номер кода; столбец 3 – параметры кода в общем виде; столбец 4 – параметры нелинейной эластичной функции в общем виде; столбец 5 – количество дополнительных переменных k, которые нужно добавить для синтеза нелинейной эластичной функции; столбец 6 –

нелинейность полученной функции; столбец 7 – максимальная нелинейность, возможная на данном векторном пространстве. Рассматриваются векторные пространства $V_6 - V_{18}$.

Таблица 2

Сводная таблица результатов

V_n	#	(u,m,t+1)	(n,t,m)	k	Nl	Nl_{max}
6	1	(4,3,2)	(6,3,1)	2	24	26
		(5,4,2)	(6,4,1)	1	16	
	3	-	-	-	-	
	4	-	-	-	-	
	5	-	-	-	-	
	6	-	-	-	-	
	7	-	-	-	-	
	8	(4,3,2)	(6,3,1)	2	24	
	9	-	-	-	-	
7	1	(5,4,2)	(7,4,1)	2	48	58
	3	-	-	-	-	
	4	-	-	-	-	
	5	-	-	-	-	
	6	-	-	-	-	
	7	-	-	-	-	
	8	-	-	-	-	
	9	-	-	-	-	
8	1	(5,4,2)	(8,4,1)	3	112	120
		(6,5,2)	(8,5,1)	2	96	
		(7,6,2)	(8,6,1)	1	64	
	3	(7,4,3)	(8,4,2)	1	64	
	4	(7,3,4)	(8,3,3)	1	64	
	5	(7,4,3)	(8,4,2)	1	64	
	6	-	-	-	-	
	7	-	-	-	-	
	8	-	-	-	-	
	9	(7,3,4)	(8,3,3)	1	64	
9	1	(6,5,2)	(9,5,1)	3	224	244
		(7,6,2)	(9,6,1)	2	192	
		(8,7,2)	(9,7,1)	1	128	
	3	(7,4,3)	(9,4,2)	2	192	
	4	(7,3,4)	(9,3,3)	2	192	
	5	(7,4,3)	(9,4,2)	2	192	
	6	(8,4,4)	(9,4,3)	1	128	
	7	-	-	-	-	
	8	(8,4,4)	(9,4,3)	1	128	
	9	(7,3,4)	(9,3,3)	2	192	
10	1	(6,5,2)	(10,5,1)	4	480	494
		(7,6,2)	(10,6,1)	3	448	
		(8,7,2)	(10,7,1)	2	384	
		(9,8,2)	(10,8,1)	1	256	
	3	(7,4,3)	(10,4,2)	3	448	
	4	-	-	-	-	
	5	(7,4,3)	(10,4,2)	3	448	
	6	(8,4,4)	(10,4,3)	2	384	
	7	-	-	-	-	
	8	(8,4,4)	(10,4,3)	2	384	
	9	-	-	-	-	
11	1	(7,6,2)	(11,6,1)	4	960	1000
		(8,7,2)	(11,7,1)	3	896	
		(9,8,2)	(11,8,1)	2	768	
		(10,9,2)	(11,9,1)	1	512	
	3	-	-	-	-	
	4	-	-	-	-	
	5	-	-	-	-	
	6	(8,4,4)	(11,4,3)	3	896	
	7	-	-	-	-	
	8	(8,4,4)	(11,4,3)	3	896	
	9	-	-	-	-	
12	1	(7,6,2)	(12,6,1)	5	1984	2016
		(8,7,2)	(12,7,1)	4	1920	
		(9,8,2)	(12,8,1)	3	1792	
		(10,9,2)	(12,9,1)	2	1536	
		(11,10,2)	(12,10,1)	1	1024	
	3-9	-	-	-	-	
13	1	(8,7,2)	(13,7,1)	5	3968	4050
		(9,8,2)	(13,8,1)	4	3840	
		(10,9,2)	(13,9,1)	3	3584	
		(11,10,2)	(13,10,1)	2	3072	
		(12,11,2)	(13,11,1)	1	2048	
	3-9	-	-	-	-	
14	1	(8,7,2)	(14,7,1)	6	8064	8126
		(9,8,2)	(14,8,1)	5	7936	
		(10,9,2)	(14,9,1)	4	7680	
		(11,10,2)	(14,10,1)	3	7168	
		(12,11,2)	(14,11,1)	2	6144	
		(13,12,2)	(14,12,1)	1	4096	
	3-9	-	-	-	-	
15	1	(9,8,2)	(15,8,1)	6	16128	16292
		(10,9,2)	(15,9,1)	5	15872	
		(11,10,2)	(15,10,1)	4	15360	
		(12,11,2)	(15,11,1)	3	14336	
		(13,12,2)	(15,12,1)	2	12288	
		(14,13,2)	(15,13,1)	1	8192	
	3-9	-	-	-	-	
16	1	(9,8,2)	(16,8,1)	7	32512	32638
		(10,9,2)	(16,9,1)	6	32256	
		(11,10,2)	(16,10,1)	5	31744	
		(12,11,2)	(16,11,1)	4	30720	
		(13,12,2)	(16,12,1)	3	28672	
		(14,13,2)	(16,13,1)	2	24576	
		(15,14,2)	(16,14,1)	1	16384	
	3	(15,5,7)	(16,5,6)	1	16384	
	4	(15,4,8)	(16,4,7)	1	16384	
	5	(15,11,3)	(16,11,2)	1	16384	
	6	-	-	-	-	
	7	(15,7,5)	(16,7,4)	1	16384	
	8	-	-	-	-	
	9	(15,10,4)	(16,10,3)	1	16384	
17	1	(10,9,2)	(17,9,1)	7	65024	65354
		(11,10,2)	(17,10,1)	6	64512	
		(12,11,2)	(17,11,1)	5	63488	
		(13,12,2)	(17,12,1)	4	61440	
		(14,13,2)	(17,13,1)	3	51344	
		(15,14,2)	(17,14,1)	2	49152	
		(16,15,2)	(17,15,1)	1	32768	
	3	(15,5,7)	(17,5,6)	2	49152	
	4	(15,4,8)	(17,4,7)	2	49152	
	5	(15,11,3)	(17,11,2)	2	49152	
	6	(16,11,4)	(17,11,3)	1	32768	
	7	(15,7,5)	(17,7,4)	2	49152	
	8	(16,5,8)	(17,5,7)	1	32768	
	9	(15,10,4)	(17,10,3)	2	49152	
18	1	(10,9,2)	(18,9,1)	8	130560	130814
		(11,10,2)	(18,10,1)	7	130048	
		(12,11,2)	(18,11,1)	6	129024	
		(13,12,2)	(18,12,1)	5	126976	
		(14,13,2)	(18,13,1)	4	122880	
		(15,14,2)	(18,14,1)	3	114688	
		(16,15,2)	(18,15,1)	2	98304	
		(17,16,2)	(18,16,1)	1	65536	
	3	(15,5,7)	(18,5,6)	3	114688	
	4	(15,4,8)	(18,4,7)	3	114688	
	5	(15,11,3)	(18,11,2)	3	114688	
	6	(16,11,4)	(18,11,3)	2	98304	
	7	(15,7,5)	(18,7,4)	3	114688	
	8	(16,5,8)	(18,5,7)	2	98304	
	9	(15,10,4)	(18,10,3)	3	114688	

Используя полученные данные, построим график зависимости нелинейности синтезированных функций от векторного пространства (рис. 1).

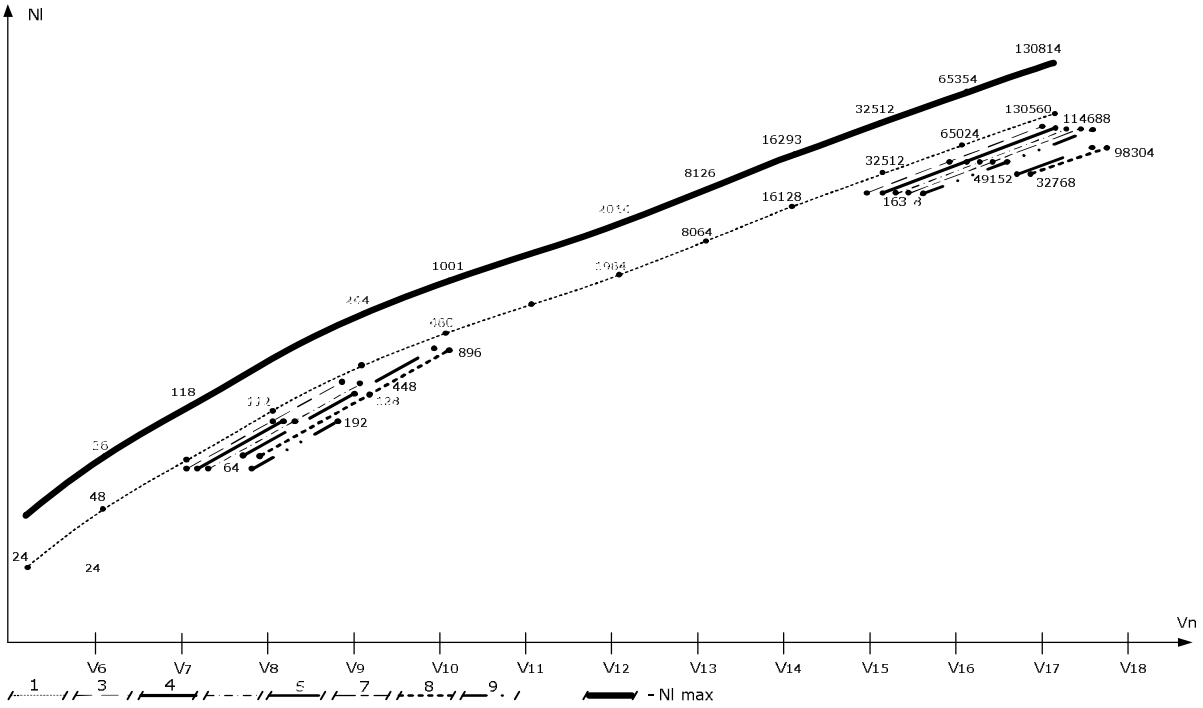

Рис. 1. График зависимости нелинейности кодов (1 – 9) от векторного пространства $V_6 - V_{18}$

Как видно из графика, наибольшей нелинейностью обладают функции, построенные с использованием кодов с проверкой на четность (код №1). На векторном поле V_8 значение нелинейности функций, построенных из кодов 3 – 9 почти в два раза ниже, чем нелинейность функции, построенной из кода проверки на четность. При этом коды 3, 5 либо не существуют, либо по ним невозможно построить эластичные функции по рассмотренному методу для векторных пространств $V_{11} - V_{15}$. Аналогично коды 4, 9 либо не существуют, либо из них невозможно построить эластичные функции по рассмотренному методу для векторных пространств $V_{10} - V_{15}$. Для кодов 6, 8 такими пространствами являются $V_{12} - V_{16}$.

Соотнесем полученные результаты с известными ранее [1], результаты сравнения сведем в табл. 3.

Таблица 3

Показатели нелинейности функции

	V_6	V_7	V_8	V_9	V_{10}	V_{11}	V_{12}	V_{13}	V_{14}	V_{15}	V_{16}
Верхняя граница	26	58	118	244	494	1000	2014	4050	8126	16292	32638
Метод модификации Себерри-Чжаня	26	–	116	–	492	–	2010	–	8120	–	32624
Методы Себерри-Чжаня, Куросавы-Сатоха	24	–	112	–	480	–	1984	–	8064	–	32512
Метод Чарпина и Пасалик	24	48	112	224	480	960	1984	3968	8064	16128	32512

Таким образом, рассмотренный метод [3] позволяет строить эластичные функции с заданными показателями нелинейности и корреляционного иммунитета. Наилучшие результаты достигаются при использовании кодов с проверкой на четность, при этом обеспечивается корреляционная иммунность $KI_f = 1$.

Другими словами, использование данного класса кодов позволяет строить функции, имеющие вид $(n+k, n-1, 1)$, где $k \le \lg_2(2^{(n-1)} - (n-1))$. Использование других блоковых кодов с бо́льшим кодовым расстоянием позволяет повысить корреляционную иммунность криптографических функций, однако это ведет к снижению их показателей нелинейности.

Выводы

В результате проведенных исследований показано, что с помощью рассмотренного метода [3] можно синтезировать эластичные булевы функции с высокими показателями нелинейности. В то же время, нелинейность полученных функций не превышает известные ранее результаты, например, пока-

затели нелинейности функций, полученных другими методами (метод модификации Собери-Чжаня). Тем не менее, рассмотренный метод позволяет синтезировать эластичные функции, обладающие корреляционным иммунитетом заданного порядка. Следовательно, можно утверждать, что рассмотренный метод перспективен для построения криптографических булевых функций с улучшенными показателями стойкости.

Перспективным направлением, по мнению авторов, является также использование недвоичных блоковых кодов для синтеза эластичных функций, разработка вычислительных алгоритмов их построения и анализа.

Список литературы

1. Кузнецов А.А. Анализ известных методов построения высоко нелинейных булевых функций / А.А. Кузнецов, Ю.А. Избенко, А.А. Юкальчук. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.nrjetix.com/fileadmin/doc/publications/articles/kuznetsov_izbenko_yukalchuk_ru.pdf.

2. Кузнецов А.А. Разработка предложение по совершенствованию симметричных средств защиты информации перспективной системы критического применения / А.А. Кузнецов, И.В. Московченко // Радіоелектронні і комп'ютерні системи. – 2008. – № 2(29). – С. 94-100.

3. Charpin P. Highly nonlinear resilient functions through disjoint codes in projective spaces / P. Charpin, E. Pasalic // Designs, codes and cryptography. – 2005. – № 37. – P. 319-346.

4. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.

5. Gupta K.C. Improved Construction of Nonlinear Resilient S-Boxes / K.C. Gupta, P. Sarkar. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.iacr.org/cryptodb/ archive/2002/ ASIACRYPT/ 242/ 242.pdf.

6. Wu C.-K. On construction of resilient function / C.-K. Wu, Ed Dawson [Электронный ресурс]. – Режим доступа к ресурсу: http://citeseer.ist.psu.edu/viewdoc/ summary? doi=10.1.1.22.1514.

7. Xiao G.-Z. A spectral characterization of correlation-immune combining functions / G.-Z. Xiao, J.L. Massey // IEEE Trans. Inform. Theory. – 1988. – Vol. IT-34(5). – P. 569-571.

8. Криптография: скоростные шифры / А.А. Молдовян и др. – СПб.: БХВ-Петербург, 2002. – 496 с.

9. Bennet C.H. Privacy amplification by public discussion /C.H. Bennet, G. Brassard, J.M. Robert // SIAM Journal on Computing. – 1988. – Vol. 24. – P. 210-229.

10. Chor B. The bit extraction problem or t-resilient functions / B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, R. Smolensky // In 26th IEEE Symposium on Foundations of Computer Science, 1985. – P. 396-407.

11. Carlet C. A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction / C. Carlet // In Advances in Cryptology – CRYPT0 2002, Lecture Notes in Computer Science, 2002. – P. 549-564.

12. Zhang X.M. Cryptographically resilient functions / X.M. Zhang, Y. Zheng // IEEE Trans. Information Theory, September, 1997. – P. 457-478.

13. Кларк Дж., мл. Кодирование с исправлением ошибок в системах цифровой связи: пер. с англ. / Дж. Кларк мл., Дж. Кейн. – М.: Радио и связь, 1987. – 392 с.

Поступила в редколлегию 24.02.2012

Рецензент: д-р техн. наук, проф. Ю.В. Стасев, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

ПОБУДОВА НЕЛІНІЙНИХ ЕЛАСТИЧНИХ ФУНКЦІЙ З ВИКОРИСТАННЯМ ДВІЙКОВИХ БЛОКОВИХ КОДІВ

О.О. Кузнецов, Л.Т. Пархуць, Г.С. Цимбал

Розглядаються методи побудови нелінійних вузлів замін симетричних криптографічних алгоритмів, досліджуються показники критерії їх ефективності. Розглядається метод побудови нелінійних еластичних функції з двійкових лінійних блокових кодів, аналізується перспективність даного методу для отримання функцій з поліпшеними показниками стійкості. Досліджуються властивості синтезованих булевих функцій за різними показниками стійкості. Оцінюється нелінійність, що досягається, та еластичність для функцій, отриманих з різних класів лінійних блокових кодів, проводяться порівняння з іншими методами синтезу й верхніми теоретичними межами для збалансованих криптографічних функцій.

Ключові слова: *криптографічні функції, нелінійність, збалансованість, еластичність, кореляційний імунітет, нелінійний вузол замін.*

THE NONLINEAR RESILIENT FUNCTIONS FROM BINARY BLOCK CODES

A.A. Kuznetsov, L.T. Parhuts', G.S. Tsymbal

Methods of creation of nonlinear nodes of changeovers of the symmetric cryptographic algorithms are considered, indexes and criteria of their efficiency are researched. The method of creation of nonlinear resilient functions from the binary linear block codes is considered, perspectivity of the given method for obtaining of functions with the improved indexes of security is analyzed. Properties of synthesizable Boolean functions on various indexes of security are researched. Nonlinearity and resilient for the functions which are received from various classes of the linear block codes is estimated. Make comparisons with other methods of synthesis and the upper theoretical boundaries for the balanced cryptography functions.

Keywords: *cryptography functions, nonlinearity, balanced, resiliency, correlation immunity, a nonlinear node of changeovers.*