

УДК 621.3.06

А.В. Казимиров, Р.В. Олейников

Харьковский национальный университет радиоэлектроники, Харьков

ИСПОЛЬЗОВАНИЕ ВЕКТОРНЫХ ФУНКЦИЙ ПРИ ГЕНЕРАЦИИ ПОДСТАНОВОК ДЛЯ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

В статье приводится описание векторных булевых функций и рассматриваются критерии отбора подстановок для симметричных криптографических примитивов в рамках данного математического аппарата. Предлагается новый метод генерации долговременных ключей для шифра ГОСТ 28147-89, который позволяет получить подстановки, принадлежащие различным классам, с нелинейностью 4, минимальной степенью 3, 4-равномерной и отсутствием фиксированных точек с оптимальной вычислительной сложностью.

Ключевые слова: векторные булевы функции, подстановки, блочный симметричный шифр, ГОСТ 28147-89.

Введение

Подстановки являются частью большинства симметричных шифров и играют основную роль в обеспечении их надежности. Блочные шифры, как одни из наиболее используемых видов симметричных шифров, в большинстве случаев являются итерационными преобразованиями над блоком открытого текста, выполняемыми под управлением ключевых данных. Итерации называются циклами, а ключ, используемый в каждом цикле, – цикловым. Каждый такой ключ вычисляется на основе ключа шифрования, используя процедуру разворачивания ключа. Циклы состоят из различных комбинаций векторных булевых функций с участием циклового ключа [1].

Существует множество атак, которые должны учитываться при проектировании шифра. К ним можно отнести различные вариации дифференциальной атаки [1, 2]: бумеранговую, невыполнимых дифференциалов, на связанных ключах, усечённых дифференциалов, высоких порядков; линейную [3], алгебраическую [4], интегральную [5] и другие. Однако, как показывает практика [6, 7, 8], в большинстве случаев основное внимание уделяется дифференциальному и линейному криптоанализу и, соответственно, выбору оптимальных подстановок с учётом данных типов атак.

Дифференциальный криптоанализ [2] предполагает наличие упорядоченных пар (α, β) таких, что случайно выбранный открытый текст M и соответствующее ему значение $M - \alpha$ после зашифрования формируют шифртексты S и S' , причем наиболее вероятной разностью шифртекстов является $S - S' = \beta$. Под « $-$ » понимается некоторая операция, обратная к введению циклового ключа. Такие упорядоченные пары (α, β) называются дифферен-

циалом. Чем выше вероятность перехода дифференциала (в то же время не равная 1), тем более эффективной является атака. Соответствующим критерием (n, m) -функции F [1], которая используется как S -блок в цикловой функции блочного шифра, является производная функции $D_a(x) = F(x) + F(x + a)$, $x, a \in \mathcal{F}_2^n$, значения которой для всех $a \neq 0$ должны быть равномерно распределены.

Линейный криптоанализ основан на Piling-up лемме и был представлен Мацуи в [3]. Основная идея заключается в следующем: для случайно выбранных битов ключа, открытого и зашифрованного текста выражение $\alpha \cdot m + \beta \cdot c + \gamma \cdot k$, где « \cdot » обозначает скалярное произведение, есть вероятность отличная от $\frac{1}{2}$. Чем больше отклонение от $\frac{1}{2}$, тем более эффективной является атака. Соответствующий критерий для S -блоков, используемых в цикловой функции шифрования, соответствует так называемым компонентным функциям [1].

Определения и обозначения

Пусть n и m – два натуральных числа. Функция $F: \mathcal{F}_2^n \mapsto \mathcal{F}_2^m$ называется (n, m) -функцией. Они используются в криптографии как нелинейные функции в псевдослучайных генераторах (поточковых шифрах) или как подстановки (S -блоки) в блочных шифрах [1]. Булевы функции f_1, \dots, f_m такие, что $F(x) = (f_1, \dots, f_m)$, называются координатными функциями F . Линейные комбинации координатных функций с ненулевыми коэффициентами называются компонентными функциями F . (n, m) -функции также известны как векторные булевы функции или S -блоки, которые часто реализуются в виде подстановок.

Преобразование Уолша некоторой (n, m) -функции отображает упорядоченную пару $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ в сумму (вычисляемую в кольце целых чисел):

$$\lambda(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x},$$

где символ “ \cdot ” обозначает скалярное произведение в векторных пространствах \mathbb{F}_2^n и \mathbb{F}_2^m . Стоит заметить, что функция $v \cdot F(x)$ является компонентной функцией F при условии $v \neq 0$. Преобразование Уолша удовлетворяет соотношению Парсеваля (Parseval):

$$\sum_{u \in \mathbb{F}_2^n} \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x} \right)^2 = 2^{2n}$$

для произвольного v . Множество, состоящее из всех значений $\lambda(u, v)$, где $u \in \mathbb{F}_2^n$ и $v \in \mathbb{F}_2^{m*} = \mathbb{F}_2^m \setminus \{0\}$, называется спектром Уолша функции F . Расширенный спектр Уолша состоит из спектра Уолша, каждый элемент которого взят по абсолютному значению.

Любая (n, m) -функция F имеет единственное представление в алгебраической нормальной форме [1]:

$$\sum_{I \subseteq \{1, \dots, n\}} a_I \left(\prod_{i \in I} x_i \right),$$

где $a_I \in \mathbb{F}_2^m$, а сумма вычисляется в \mathbb{F}_2^m .

Алгебраическая степень (n, m) -функции F равна $\max\{|I| \mid a_I \neq 0\}$. Векторные функции, используемые в криптографии, должны иметь высокую алгебраическую степень, чтобы обеспечивать защиту от различных типов атак (например от дифференциальной атаки высоких порядков) [9]. Функция называется аффинной, если её алгебраическая степень равна 1 и квадратичной – в случае второй [1].

Любая (n, n) -функция F имеет единственное одномерное представление над полем \mathbb{F}_2^n со степенью, не превышающей $2^n - 1$:

$$F(x) = \sum_{j=0}^{2^n-1} \delta_j x^j, \quad \delta_j \in \mathbb{F}_2^n.$$

Пусть $w_2(j)$ – количество ненулевых бит в двоичном представлении числа j . Тогда функция F имеет алгебраическую степень, равную $\max\{w_2(j) \mid \delta_j \neq 0\}$.

Ниже приведена лемма, также известная как критерий Эрмита (Hermite) [10], которая часто ис-

пользуется для определения перестановочного полинома над конечным полем.

Лемма 1. Пусть p – характеристика поля \mathbb{F}_q .

Полиномом $F \in \mathbb{F}_q[x]$ является перестановочным тогда и только тогда, когда выполняются следующие два условия:

- F имеет ровно один корень в поле \mathbb{F}_q ;
- для всех $t = \{1, \dots, q-2\}$ и $t \neq 0 \pmod{p}$ полином $F(x)^t \pmod{x^q - x}$ имеет степень, не превышающую $q-2$.

Другими словами, функция называется перестановочной тогда и только тогда, когда генерирует перестановку элементов поля.

Функция $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ называется линейной тогда и только тогда, когда F является линейным полиномом над полем \mathbb{F}_{2^n} :

$$F(x) = \sum_{i=0}^{n-1} c_i x^{2^i}, \quad c_i \in \mathbb{F}_{2^n}.$$

Сумма линейной функции и константы называется аффинной функцией. Если m делит n , тогда любая (n, m) -функция может быть представлена как отображение поля \mathbb{F}_{2^n} в себя, так как \mathbb{F}_{2^m} является подполем поля \mathbb{F}_{2^n} . Поэтому функция имеет уникальное представление вида:

$$F(x) = \text{tr}_{n/m} \left(\sum_{j=0}^{2^n-1} \delta_j x^j \right), \quad \delta_j \in \mathbb{F}_{2^n},$$

где $\text{tr}_{n/m}(x) = x + x^{2^m} + x^{2^{2m}} + x^{2^{3m}} + \dots + x^{2^{n-m}}$ – след из поля \mathbb{F}_{2^n} в \mathbb{F}_{2^m} .

(n, m) -функция F является сбалансированной тогда и только тогда, когда её компонентные функции являются сбалансированными (т.е. вес Хемминга равен 2^{n-1}) [1].

Нелинейность $nl(F)$ (n, m) -функции F есть минимальное расстояние Хемминга между всеми компонентными функция F и всеми аффинными функциями с n переменными:

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_2^{m*}; u \in \mathbb{F}_2^n} \left\{ \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x} \right| \right\}.$$

Критерий нелинейности определяет уровень защищённости S-блока от линейного криптоанализа [1, 3, 11, 12].

В следующей теореме приводится граница значения нелинейности, также известная как граница Сидельникова-Чабауда-Вауденая (Sidelnikov-Chabaud-Vaudena) [12].

Теорема 1. Пусть n и m натуральные числа такие, что $m \geq n-1$. Пусть F произвольная (n, m) -функция. Тогда:

$$nl(F) \leq 2^{n-1} - \frac{1}{2} \sqrt{3 \times 2^n - 2 - 2 \frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}}.$$

При $m = n-1$ неравенство сводится к $nl(F) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$, которое известно как граница радиуса покрытия (covering radius bound).

Векторная булева функция является бент-функцией, если для всех значений $v \neq 0$ и u преобразование Уолша принимает значения $\pm 2^{\frac{n}{2}}$. Если значения принадлежат множеству $\left\{0, \pm 2^{\frac{n+1}{2}}\right\}$, то такая функция называется почти бент (ПБ) (almost bent).

С другой стороны, любая (n, m) -функция F является бент-функцией тогда и только тогда, когда её производная функция $(D_a(x) = F(x) + F(x+a), x, a \in \mathbb{F}_2^n)$ сбалансирована [1]. По этой причине бент-функции также называются совершенно нелинейными (СН) (perfect nonlinear).

Любая (n, m) -функция F является δ -равномерной, если для любого $a \in \mathbb{F}_2^{n*}$ и $b \in \mathbb{F}_2^m$ уравнение $D_a(x) = b$ имеет не более δ решений [1, 13]. Функция F называется почти совершенно нелинейной (ПСН) (almost perfect nonlinear (APN)), если $\delta = 2$. Нижняя граница δ равна 2^{n-m} и равна ей тогда и только тогда, когда F является совершенно нелинейной [1, 13].

Две функции $F, G: \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ называются расширенно аффинно (РА) эквивалентными (extended affine (EA) equivalent), если существуют такие аффинно-перестановочные функции $A_1(x) = L_1(x) + c_1, A_2 = L_2(x) + c_2$ и произвольная линейная функция $L_3(x)$, что [14, 15]:

$$F = A_1(G(A_2(x))) + L_3(x) = A_1 \circ G \circ A_2(x) + L_3(x).$$

При выполнении условия $L_3 = \text{const}$ функции F и G называются аффинно-эквивалентными; а при $L_3 = 0, c_1 = 0, c_2 = 0$ – линейно-эквивалентными.

В работе [16] функции рассматриваются в более общем представлении – в виде функции $G_F(x, y) = (\{x, y\} : y = F(x))$. Пусть $\mathcal{L}(x, y)$ – некоторая аффинная перестановочная функция, отображающая векторное пространство \mathbb{F}_2^{2n} в себя, тогда:

$$\mathcal{L}(x, y) = (L_1(x) + L_2(y), L_3(x) + L_4(y))$$

для некоторых аффинных функций L_1, L_2, L_3, L_4 из \mathbb{F}_2^n в себя. Другими словами, $\mathcal{L}(x, y)$ аффинная перестановочная функция, если система

$$\begin{cases} L_1(x) + L_2(y) = 0, \\ L_3(x) + L_4(y) = 0 \end{cases}$$

имеет лишь одно решение [1, 16].

Две функции F и G называются Карлет-Шарпин-Зиновьев (КШЗ) (Carlet-Charpin-Zinoviev (CCZ))-эквивалентными, если существует аффинная перестановка $\mathcal{L}: \mathbb{F}_2^{2n} \mapsto \mathbb{F}_2^{2n}$ такая, что $G_F = \mathcal{L}(G_G)$. Две функции F и G КШЗ-эквивалентны тогда и только тогда, когда для некоторой аффинной перестановки $\mathcal{L}(x, y) \subset \mathbb{F}_2^{2n}$:

$$F(x) = F_2 \circ F_1^{-1}(x),$$

где $F_1(x) = L_1(x) + L_2 \circ G(x)$ перестановочная функция, а $F_2(x) = L_3(x) + L_4 \circ G(x)$ – произвольная.

Для КШЗ- и РА-эквивалентных функций инвариантными остаются следующие криптографические свойства: расширенный спектр Уолша (ПБ, СН, нелинейность), δ -равномерность (ПСН). Алгебраическая степень сохраняется только для РА-эквивалентных функций. Таким образом, КШЗ-эквивалентность является более общим случаем РА-эквивалентности и обратных функций [1, 15].

К подстановкам, применяемым в блочных шифрах, дополнительно ко всем вышеперечисленным критериям необходимо добавить следующие: отсутствие фиксированных точек и высокий алгебраический иммунитет. Более подробно эти критерии описаны в работе [17]. На сегодняшний день нет однозначного набора критериев для идеального S-блока. Поэтому далее приводятся результаты, ориентированные на достижение максимальных показателей δ -равномерности и расширенного спектра Уолша.

Генерация подстановок с заданными свойствами

Известно несколько классов степенных ПСН функции. В табл. 1 приводятся все известные на сегодняшний день экспоненты d вплоть до эквивалентности такие, что функция x^d является ПСН над полем \mathbb{F}_2^n . Для чётного n Голд (Gold), Касами (Kasami), Вэшл (Welch) и Ниho (Niho) функции также являются ПБ [1]. Когда n четное, обратные функции являются дифференциально 4-распределёнными перестановками [18]. Данный вид функций вместе с аффинным преобразованием использовался при выборе подстановок в алгоритмах шифрования AES [19] и Лабиринт [20]. Существует и множество других нестепенных классов функций, которые ранее были рассмотрены в [1, 21].

Таблица 1

Известные степенные ПСН функции x^d над полем F_{2^n}

Название	Экспонента d	Условие	Источник
Голд	$2^i + 1$	$\text{НОД}(i, n) = 1$	[22]
Касами	$2^{2i} - 2^i + 1$	$\text{НОД}(i, n) = 1$	[23]
Вэлш	$2^t + 3$	$n = 2t + 1$	[24]
Нихо	$2^t + 2^{\frac{t}{2}} - 1$	$n = 2t + 1, t - \text{чётное}$	[25]
	$2^t + 2^{\frac{3t+1}{2}} - 1$	$n = 2t + 1, t - \text{нечётное}$	
Обратные	$2^{2t} - 1$	$n = 2t + 1$	[18]
Доббертин	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[26]

До недавнего времени считалось, что ПСН перестановочных функций для чётного значения n не существует [1]. Однако в 2010 году была представлена работа [27], где авторы привели пример такой функции для $n = 6$. Для поиска использовался метод, использующий результаты теории кодирования, КШЗ-эквивалентность и значительное количество вычислений.

Теорема 1. Пусть α – примитивный элемент поля F_{2^6} . Тогда ПСН функция

$$H(x) = \alpha x^3 + \alpha^5 x^{10} + \alpha^4 x^{24}$$

является КШЗ-эквивалентной ПСН перестановочной функции над полем F_{2^6} [30].

Например, для функции

$$\mathcal{L}(x, y) = (\text{tr}_{6/3}(\alpha^4 x) + \alpha \text{tr}_{6/3}(y), \text{tr}_{6/3}(\alpha x) + \alpha \text{tr}_{6/3}(\alpha^4 y)),$$

где $\text{tr}_{6/3}(x) = x + x^2^3$, $y = H(x)$ функция

$G_F = \mathcal{L}(G_H)$ является ПСН перестановочной. Однако на сегодняшний день остаётся открытым вопрос о существовании ПСН перестановок для $n \geq 8$.

Исследование подстановок в виде векторных функций предоставляет возможность значительно оптимизировать формирование узлов замены сим-

метричных криптографических примитивов. Например, позволяет находить целые классы функции со схожими свойствами, использование которых позволяет сократить время поиска оптимальной подстановки. Так, в работах [28, 29] были классифицированы все 4-битные перестановки с оптимальными показателями. Оптимальной считалась биективная подстановка с нелинейностью, равной 4 и 4-равномерная [28]. Всего получилось 16 различных векторных булевых функций, не являющихся аффино-эквивалентными. В криптографии, помимо линейных и дифференциальных показателей, важным является критерий минимальной степени компонентных функций. Для 4-битной перестановки это значение должно быть равно 3. В табл. 2 приведены 8 из 16 векторных булевых функций, удовлетворяющих данному критерию. Переменная g является мультипликативным генератором поля F_{2^4} с примитивным полиномом $x^4 + x + 1$.

Стоит заметить, что полиномы являются КШЗ-эквивалентными. Взаимосвязь между функциями представлена ниже:

$$F_1 \sim \text{CCZ } F_3; \quad F_2 \sim \text{CCZ } F_4;$$

$$F_5 \sim \text{CCZ } F_6 \sim \text{CCZ } F_7.$$

Таблица 2

Полиномиальное представление оптимальных подстановок, принадлежащих различным классам

	Полином
F_1	$x^{14} + g^{11} x^{13} + g x^{12} + g^3 x^{11} + g^5 x^9 + g^7 x^8 + g^8 x^7 + g^4 x^6 + g^{11} x^5 + g^2 x^4 + g^4 x^3 + g^{11} x^2$
F_2	$x^{14} + g^{11} x^{13} + g^7 x^{12} + g x^{11} + g^8 x^{10} + g^{13} x^9 + g^{11} x^8 + g^2 x^6 + g x^5 + g^2 x^4 + g^7 x^3 + g x^2 + g^8 x$
F_3	$x^{14} + g^{13} x^{13} + g^9 x^{12} + g^6 x^{11} + g^{10} x^{10} + g^7 x^9 + g^{10} x^8 + g^7 x^7 + g^8 x^6 + g^{12} x^5 + g^{12} x^4 + x^3 + g^{11} x^2 + g^5 x$
F_4	$x^{14} + g^4 x^{13} + g^3 x^{12} + g^2 x^{11} + x^{10} + g^{11} x^9 + g^2 x^8 + g x^7 + g^2 x^6 + g^9 x^5 + g^4 x^4 + g x^3 + g^{12} x^2 + g^{11} x$
F_5	$x^{14} + g x^{13} + g^9 x^{12} + g x^{11} + g^7 x^{10} + g^6 x^7 + g^{10} x^6 + g x^5 + g^8 x^4 + g^2 x^3 + g^6 x^2 + g^9 x$
F_6	$x^{14} + g x^{13} + x^{12} + g^7 x^{11} + g^{13} x^{10} + g x^9 + g^{11} x^8 + g^{14} x^7 + g^3 x^6 + g^6 x^5 + g x^4 + g^{14} x^3 + g^{14} x^2 + g^9 x$
F_7	$x^{14} + g^{10} x^{13} + g x^{12} + g^4 x^{11} + g^{14} x^{10} + g^4 x^9 + g^5 x^8 + g^2 x^7 + g^9 x^6 + g^4 x^5 + g^8 x^4 + g^{14} x^3 + g^5 x^2 + x$
F_8	$x^{14} + g^{12} x^{13} + g^8 x^{12} + g^8 x^{11} + g^{14} x^{10} + g x^9 + g^8 x^8 + g^{14} x^7 + g^6 x^6 + x^5 + g^{14} x^4 + g^{12} x^3 + g x^2 + g^{14} x$

Отсюда и далее под оптимальной понимается подстановка [17]:

- а) биективная;
- б) 4-равномерная;
- в) с нелинейностью 4;
- г) с минимальной степенью 3;
- д) отсутствием фиксированных точек (нет циклов длиной 1).

На основе функций, описанных в табл. 2, предлагается методика генерации долговременных ключевых элементов (ДКЭ) для шифра ГОСТ 28147-89 [30]. На первом шаге каждой из 8 подстановок ДКЭ (K_1, \dots, K_8) ставится в соответствие векторная булева функция F_1, \dots, F_8 .

Количество соответствий равно $8! = 4320$. Далее, к каждому полиному последовательно применяются различные аффинно-эквивалентные преобразования до тех пор, пока функция (подстановка) не будет удовлетворять пункту д).

Количество аффинно-эквивалентных функций равно

$$\left(\prod_{i=1}^n (2^n - 2^{i-1}) \right)^2 \cdot 2^{2n}.$$

Для случая $n=4$ общее количество ДКЭ, которые можно получить при помощи данного метода, не превышает

$$\left(\prod_{i=1}^4 (2^4 - 2^{i-1}) \right)^2 \cdot 2^8 \cdot 8! \approx 2^{51}$$

и равно ему в случае отсутствия пункта д). Как было описано ранее, аффинное преобразование сохраняет свойства а)-г).

Таким образом, предлагаемый метод позволяет сократить время, необходимое на генерацию и проверку криптографических параметров подстановок для шифра ГОСТ 28147-89 за счёт заранее выбранных векторных булевых функций с параметрами а - г. Пример ДКЭ с оптимальными показателями, сгенерированный по предложенному методу, представлен в табл. 3.

Таблица 3

Пример долговременных ключевых элементов с оптимальными показателями

	Ключ
K_1	[5, 11, 13, 10, 8, 4, 1, 0, 6, 12, 3, 15, 2, 9, 7, 14]
K_2	[7, 8, 12, 10, 2, 1, 15, 14, 11, 13, 5, 9, 0, 3, 6, 4]
K_3	[15, 14, 7, 5, 3, 13, 9, 2, 10, 6, 11, 1, 8, 0, 12, 4]
K_4	[15, 8, 9, 14, 1, 4, 13, 11, 3, 5, 6, 12, 0, 2, 7, 10]
K_5	[5, 10, 6, 15, 8, 4, 2, 3, 9, 7, 13, 0, 14, 1, 12, 11]
K_6	[7, 9, 12, 8, 10, 2, 13, 14, 0, 5, 4, 6, 3, 15, 1, 11]
K_7	[8, 14, 11, 5, 1, 4, 7, 6, 13, 2, 9, 15, 3, 10, 12, 0]
K_8	[13, 14, 6, 10, 2, 15, 0, 5, 12, 1, 11, 4, 9, 8, 3, 7]

Выводы

Применение математического аппарата векторных булевых функций позволяет реализовать эффективную методику формирования нелинейных подстановочных конструкций для симметричных криптографических примитивов с оптимальными показателями. Использование ПСН и ПБ функций позволяет добиться максимально возможных параметров, что необходимо для защиты от дифференциального и линейного криптоанализа.

Применение методики для генерации долговременных ключевых элементов ГОСТ 28147-89 обеспечивает формирование перестановок, принадлежащих различным аффинно-эквивалентным классам с нелинейностью 4, минимальной степенью 3, 4-равномерной и отсутствием фиксированных точек, что позволяет обеспечить значительный запас стойкости к известным видам криптоанализа.

Список литературы

1. Carlet C. *Vectorial Boolean Functions for Cryptography*. [Электронный ресурс] / C. Carlet. – URL <http://www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf>.
2. Biham E. *Differential Cryptanalysis of DES-like Cryptosystems* / E. Biham, A. Shamir // *Journal of Cryptology*. – 1991. – Vol 4, No.1. – P. 3-72.
3. Matsui M. *Linear cryptanalysis method for DES cipher* / M. Matsui // *Advances in Cryptology - EUROCRYPT'93*, no. 765 in *Lecture Notes in Computer Science*. Springer-Verlag, 1994. – P. 386-397.
4. Courtois N. *Cryptanalysis of block ciphers with overdefined systems of equations* / N. Courtois, J. Pieprzyk // *Advances in cryptology-ASIACRYPT 2002, Lecture Notes in Computer Science 2501*. – Springer, 2003. – P. 267-287.
5. Knudsen L. *Integral Cryptanalysis* / L. Knudsen, D. Wagner // *Proceedings of Fast Software Encryption - FSE'02*, number 2365 in *Lecture Notes in Computer Science*. – Springer-Verlag, 2002. – P. 112-127.
6. Preneel B. *Final report of European project number IST-1999-12324, named New European Shames for Signa-*

tures, Integrity, and Encryption [Electronic resource] / B. Preneel, A. Biryuov, C. De Canniere, etc. Mode of access : WWW.URL: <https://www.cosic.esat.kuleuven.be/messie/Book015.pdf> – Last access: 2012. – Title from the screen.

7. CRYPTREC Report 2002 [Electronic resource] / Mode of access : WWW.URL: Information-technology Promotion Agency, Japan http://cryptrec.nict.go.jp/eng_info_page/cryptrec_03_0829_c02_report.htm – Last access: 2010. – Title from the screen.

8. Положення про проведення відкритого конкурсу криптографічних алгоритмів [Електронний ресурс] / ДССЗІУ. – Режим доступу: WWW.URL: http://www.dstzsi.gov.ua/dstzsi/control/uk/publish/article?art_id=48383&cat_id=38710 - Последний 05.06.2010 г. – Загл. с экрана.

9. Lars R. Knudsen. Truncated and Higher Order Differentials / Lars R. Knudsen // In Bart Preneel, editor, FSE, volume 1008 of LNCS/ – Springer, 1994. – P. 196-211.

10. Lidl R. 'Finite Fields' / R. Lidl, H. Niederreiter // Cambridge University Press (Revised Edition), 1994.

11. Carlet C. On cryptographic complexity of Boolean functions / C. Carlet. – To appear in the proceedings of Fq6.

12. Chabaud F. Links between Differential and Linear Cryptanalysis / F. Chabaud, S. Vaudenay // EUROCRYPT'94, Advances in Cryptology, Lecture Notes in Computer Science 950. – Springer Verlag. – 1995. – P. 356-365.

13. Beth T. On almost perfect nonlinear permutations / T. Beth, C. Ding // Advances in Cryptology – Eurocrypt' 93, Lecture Notes in Computer Science, 765. – New York, Springer-Verlag. 1994. – P. 65-76.

14. Budaghyan L. Constructing new APN functions from known ones / L. Budaghyan, C. Carlet, G. Leander. – To appear in Finite Fields and Applications, 2008.

15. Budaghyan L. New Classes of Almost Bent and Almost Perfect Nonlinear Polynomials / L. Budaghyan, C. Carlet, A. Pott // Proceedings of the Workshop on Coding and Cryptography 2005. – Bergen, 2005. – P. 306-315.

16. Carlet C. Codes, bent functions and permutations suitable for DES-like cryptosystems / C. Carlet, P. Charpin, V. Zinoviev // Designs, Codes and Cryptography, 15(2). – 1998. – P. 125-156.

17. Oliynykov R. An impact of S-box Boolean function properties to strength of modern symmetric block ciphers / R. Oliynykov, O. Kazymyrov // Радіотехніка. – 2011. – №166. – С. 11-17.

18. Nyberg K. Perfect non-linear S-boxes / K. Nyberg // Advances in Cryptology, EUROCRYPT' 91. – Springer Verlag, Lecture Notes in Computer Science 547. – 1992. – P. 378-386.

19. AES-FIPS. Specification for the Advanced Encryption Standard (AES), Federal Information Processing Stand-

ards Publication 197, 2001. [Электронный ресурс]. – URL <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

20. Головашич С.А. Алгоритм блочного симметричного шифрования «Лабиринт» [Текст] / С.А. Головашич. – Х., 2007. – 46 с.

21. Тужилин М.Э. Почти совершенные нелинейные функции / М.Э. Тужилин // Прикладная дискретная математика. – 2009. – №3(5). – С. 14-20.

22. Gold R. Maximal recursive sequence with 3-valued recursive cross-correlation functions / R. Gold // IEEE Transactions on Information Theory. – 1968. – V. 14, No. 1. – P. 154-156.

23. Kasami T. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes / T. Kasami // Information and Control. – 1971. – V. 18. – P. 369-394.

24. Dobbertin H. Almost perfect nonlinear power functions over $GF(2^n)$: The Welch case / H. Dobbertin // IEEE Transactions on Information Theory. – 1999. – V. 45, No. 4. – P. 1271-1275.

25. Dobbertin H. Almost perfect nonlinear power functions over $GF(2^n)$: The Niho case / H. Dobbertin // International J. of Computer and Information Sciences. – 1999. – V. 151. – P. 57-72.

26. Dobbertin H. Almost perfect nonlinear power functions over $GF(2^n)$: A new case for n divisible 5 / H. Dobbertin // Proc. of Finite Fields and Applications Fq5. – Springer Verlag, 2001. – P. 113-121.

27. Browning K. An APN permutation in dimension 6 / K. Browning, J.F. Dillon, M. McQuistan, A.J. Wolfe // Proceedings of Conference Finite Fields and Applications Fq9, Contemporary Mathematics 518. – 2009. – P. 33-42.

28. Leander G. On the Classification of 4 Bit S-Boxes / G. Leander, A. Poschmann // In C. Carlet and B. Sunar (Eds.): WAIFI 2007, LNCS 4547. – Springer (2007). – P. 159-176.

29. Markku-Juhani O. Saarinen. Cryptographic Analysis of All 4×4 -Bit S-Boxes / Markku-Juhani O. Saarinen // Selected Areas in Cryptography. – 2011. – P. 118-133.

30. ГОСТ 28147-89. Системи обробки інформації. Захита криптографіческой. Алгоритм криптографіческого преобразования ГОСТ 28147-89 [Текст]. – М. : Изд-во стандартов, 1989.

Поступила в редколлегию 12.06.2012

Рецензент: д-р техн. наук, проф. И.Д. Горбенко, Харьковский национальный университет радиоэлектроники, Харьков.

ВИКОРИСТАННЯ ВЕКТОРНИХ ФУНКЦІЙ ПРИ ГЕНЕРАЦІЇ ПІДСТАНОВОК ДЛЯ СИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЮВАНЬ

О.В. Казимиров, Р.В. Олійников

У статті приводиться опис векторних бульових функцій и розглядаються критерії відбору підстановок для симетричних криптографічних примітивів у рамках даного математичного апарату. Пропонується новий метод генерації довгострокових ключів для шифру ГОСТ 28147-89, який дозволяє отримати підстановки, які належать різним класам, з нелінійністю 4, мінімальним степенем 3, 4-рівномірністю і відсутністю фіксованих точок з оптимальною обчислювальною складністю.

Ключові слова: векторні бульови функції, підстановки, блоковий симетричний шифр, ГОСТ 28147-89.

VECTORIAL BOOLEAN FUNCTIONS APPLICATION IN SUBSTITUTIONS GENERATION FOR SYMMETRIC CRYPTOGRAPHIC TRANSFORMATION

A.V. Kazimirov, R.V. Olejnikov

The descriptions of the vectorial Boolean functions as well as criteria for substitutions and a new method for S-box generation for the cipher GOST 28147-89 with optimal computational complexity are given. The method provides substitutions that belong to different affine classes, with nonlinearity 4, minimum degree 3, 4-uniform and without fixed points.

Keywords: vectorial Boolean functions, substitutions, block ciphers, GOST 28147-89.