УДК 004.056.55

СИЛЬНО НЕЛИНЕЙНЫЕ ПОДСТАНОВКИ: МЕТОД СИНТЕЗА S-БЛОКОВ, ОБЛАДАЮЩИХ МАКСИМАЛЬНОЙ 4-НЕЛИНЕЙНОСТЬЮ

Соколов А.В., Красота Н.И.

Одесский национальный политехнический университет,
65044, Украина, г. Одесса, пр-т Шевченко, 1.
radiosquid@gmail.com

СИЛЬНО НЕЛІНІЙНІ ПІДСТАНОВКИ: МЕТОД СИНТЕЗУ S-БЛОКІВ, ЩО ВОЛОДІЮТЬ МАКСИМАЛЬНОЮ 4-НЕЛІНІЙНІСТЮ

Соколов А.В., Красота Н.І.

Одеський національний політехнічний університет,
65044, Україна, м. Одеса, пр-т Шевченка, 1.
radiosquid@gmail.com

VERY NONLINEAR PERMUTATIONS: SYNTHESIS METHOD FOR S-BOXES WITH MAXIMAL 4-NONLINEARITY

Sokolov A.V, Krasota N.I.

Odessa National Polytechnic University,
ave. Shevchenko, 1, 65044, Odessa, Ukraine.
radiosquid@gmail.com

Аннотация. Одним из наиболее важных компонентов современных блочных симметричных криптоалгоритмов является S-блок. Так, качество криптопреобразования в целом во многом базируется на свойствах применяемого в нем S-блока, а именно: лавинный эффект, корреляционный иммунитет и, в особенности, нелинейность. За время развития теории криптографии было предложено несколько способов определения нелинейности S-блоков, таких как алгебраическая степень нелинейности и расстояние нелинейности. Тем не менее, все они учитывают только описание S-блока с помощью математического аппарата булевых функций. Однако, криптоаналитик не стеснен в используемых описаниях шифра, в частности, с помощью функций многозначной логики. В этом свете актуальным является исследование нелинейных свойств компонентных функций многозначной логики S-блоков подстановки. В настоящей статье предложена методика оценки 4-нелинейности функций многозначной логики на основе преобразования Виленкина-Крестенсона, отражающая степень равномерности спектра Виленкина-Крестенсона. Проведенные исследования позволили установить, что изученные современные конструкции S-блоков не обладают удовлетворительными свойствами с точки зрения 4-нелинейности. Данное обстоятельство продиктовало задачу построения нового метода синтеза 4-нелинейных S-блоков, которая нашла свое решение в данной статье.

Ключевые слова: S-блок, нелинейность, многозначная логика.

Анотація. Одним із найбільш важливих компонентів сучасних блокових симетричних криптоалгоритмів є S-блок. Так, якість криптоперетворення у цілому багато в чому базується на властивостях застосовуваного в ньому S-блока, а саме: лавинний ефект, кореляційний імунітет, і особливо, нелінійність. За час розвитку теорії криптографії було запропоновано кілька способів визначення нелінійності S-блоків, таких як алгебраїчна степінь нелінійності і відстань нелінійності. Проте всі вони враховують тільки опис S-блока за допомогою математичного апарата булевих

функцій. Однак, криптоаналітик не обмежений у використовуваних описах шифру, зокрема, за допомогою функцій багатозначної логіки. Таким чином, актуальним є дослідження нелінійних властивостей компонентних функцій багатозначної логіки S-блоків підстановки. У цій статті запропонована методика оцінки 4-нелінійності функцій багатозначної логіки на основі перетворення Віленкіна-Крестенсона, що відображає степінь рівномірності спектра Віленкіна-Крестенсона. Проведені дослідження дозволили встановити, що досліджені сучасні конструкції S-блоків не володіють задовільними властивостями з точки зору 4-нелінійності. Така обставина продиктувала завдання побудови нового методу синтезу 4-нелінійних S-блоків, яка знайшла своє рішення в даній статті.

Ключові слова: S-блок, нелінійність, багатозначна логіка.

Abstract. One of the most important components of modern block symmetric cryptographic algorithms is the S-box. Thus, the quality of cryptographic transform is in general largely dependent on the properties of used S-box, such as the avalanche effect, correlation immunity, and in particular, nonlinearity. During the development of the theory of cryptography, several methods for determining the nonlinearity of S-boxes have been proposed, such as the algebraic degree of nonlinearity and the distance of nonlinearity. Nevertheless, they all take into account only the description of the S-box using the mathematical apparatus of Boolean functions. But, the cryptanalyst is not constrained in the used cipher description methods, in particular with the application of functions of many-valued logic. In this respect, it is relevant to research the nonlinear properties of the component many-valued functions of S-boxes. In this paper, we propose a technique for estimating the 4-nonlinearity of many-valued logic functions based on the Vilenkin-Chrestensen transform, which considers the degree of uniformity of the Vilenkin-Chrestensen spectrum. The performed research made it possible to understand that many widely used modern constructions of S-boxes do not satisfy the high nonlinearity criterion from the point of view of 4-nonlinearity. This circumstance defined the task of constructing a new method for the synthesis of 4-nonlinear S-boxes, which found its solution in this paper.

Key words: S-box, nonlinearity, many-valued logic.

Памяти д.т.н., проф.
Мазуркова Михаила Ивановича

Введение и постановка задачи. Нелинейные S-блоки являются основным компонентом блочных симметричных шифров [1], к которым предъявляются строгие критерии качества. Одним из таких критериев является нелинейность S-блока. В настоящее время самым универсальным методом измерения нелинейности является её определение через расстояние до объекта, имеющего наиболее простое математическое описание. В качестве такого объекта в современной криптографии принято множество двоичных аффинных функций [1] в виду максимальной линейности (отсутствие операции конъюнкции) их алгебраической нормальной формы. Тем не менее, при атаке на алгоритм шифрования криптоаналитик не стеснен в используемых средствах и может использовать аппроксимацию элементов шифра любыми доступными способами, в том числе и методами многозначной логики. Таким образом, при конструировании S-блоков подстановки имеет смысл рассматривать не только двоичные аффинные функции, но и аффинные функции многозначной логики, через которые может быть представлен S-блок данного размера. Тем не менее, методов, позволяющих оценить степень удаленности двоичного S-блока от аффинных функций многозначной логики на сегодняшний день не существует. Тем более, не существует метода синтеза S-блоков подстановки, обладающих максимальной нелинейностью как в смысле удаленности от двоичных аффинных функций, так и в смысле удаленности от аффинных функций многозначной логики.

Целью настоящей статьи является разработка методики исследования нелинейных свойств S-блоков подстановки на основе четверичного преобразования Виленкина-Крестенсона, а также метода синтеза S-блоков подстановки длины $N=16$, обладающих максимальным удалением как от двоичных, так и от четверичных аффинных функций.

Определение двоичной нелинейности S-блока подстановки является общепринятым [2] и сводится к нахождению минимума среди расстояний Хэмминга между компонентными

булевыми функциями S-блока F_i и множеством аффинных булевых функций, т.е. кодовыми словами аффинного $A(N,k)$-кода

$$N_S = \min(dist(F_i, A_j)), \quad i = \overline{1,k}, \quad j = 1, 2^{k+1} . \tag{1}$$

Определение 1 [3]. Для произвольного натурального k, аффинным $A(N,k)$-кодом длины $N = 2^k$ называется множество всех строк $\{A_j\}$ тех булевых функций, степень нелинейности которых не превышает 1.

Кодовыми словами аффинного $A(N,k)$-кода фактически являются строки матрицы Адамара и их инверсии [4], таким образом, расстояние нелинейности связано со значениями коэффициентов преобразования Уолша-Адамара компонентных булевых функций. А именно, это расстояние равняется величине

$$N_f = 2^{k-1} - \frac{1}{2} \max_{\omega \in Z_2^k} |W_F(\omega)|, \quad \omega = 0,1,...,2^k - 1, \tag{2}$$

где W_F — коэффициенты преобразования Уолша-Адамара.

Учитывая равенство Парсеваля, а также структурные свойства преобразования Уолша-Адамара, становится понятно, что для того чтобы нелинейность булевой функции была максимальной, необходимо чтобы модули её коэффициентов преобразования Уолша-Адамара были распределены как можно более равномерно. Другими словами, чтобы данная булева функция «содержала в себе» приблизительно равное количество каждой из аффинных функций.

Таким образом, такая характеристика S-блоков, как двоичное расстояние нелинейности полностью зависит от аффинного кода и введение расстояния нелинейности для функций многозначной логики требует рассмотрения объекта, являющегося многозначным аналогом аффинного кода.

Функции Виленкина-Крестенсона и определение 4-нелинейности. В теории сигналов в качестве ортогонального преобразования наиболее часто рассматривают системы ортогональных функций Виленкина-Крестенсона, которые являются обобщением функций Уолша на многозначный случай [5].

Функции Виленкина-Крестенсона могут быть определены, в частности, через определение аффинного кода функций многозначной логики.

Определение 2 [6]. Функцией q-значной логики (далее q-функция) k переменных называется отображение $\{0,1,2,3...,q-1\}^k \to \{0,1,2,3...,q-1\}$.

Очевидно, S-блоки, распространенной на практике длины $N = 16$, могут быть однозначно определены с помощью функций 4-логики, таким образом, в настоящей статье введено и рассматривается определение 4-нелинейности. Тем не менее, для других длин S-блоков определения q-нелинейности могут быть введены аналогичным образом, если их длина N может быть представлена в виде $N = q^k$, $k \in N$.

Подобно булевым функциям, 4-функции также могут быть однозначным образом представлены в алгебраической нормальной форме, т.е. в виде полинома, содержащего операции умножения и сложения, которые определяются следующими таблицами арифметических операций по mod4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

,

·	0	1	2	3
0	0	0	0	0
1	0	3	2	1
2	0	2	0	2
3	0	1	2	3

. (3)

Например, для значения $k=1$, запишем общий вид алгебраической нормальной формы 4-функции

$$f(x_1)=a_0+a_1x_1+a_2x_1^2+a_3x_1^3, \tag{4}$$

в то время как для случая $k=2$

$$\begin{aligned} f(x_1,x_2)=a_0+a_1x_1+a_2x_2+a_3x_1x_2+a_4x_1^2+a_5x_2^2+a_6x_1^2x_2+a_7x_1x_2^2+a_8x_1^2x_2^2+ \\ +a_9x_1^2x_2^3+a_{10}x_1^3x_2^2+a_{11}x_1^3x_2^3+a_{12}x_1^3+a_{13}x_2^3+a_{14}x_1x_2^3+a_{15}x_1^3x_2, \end{aligned} \tag{5}$$

где $a_i\in\{0,1,2,3\}$.

В соответствии с **Определением 1** аффинными являются все 4-функции, имеющие вид:

$$f(x_1,\ldots,x_k)=a_0+a_1x_1+a_2x_2+\ldots+a_kx_k\,(\mathrm{mod}\,4)=\sum_{i=1}^{k}a_ix_i\,(\mathrm{mod}\,4)+a_0, \tag{6}$$

где $a_i\in\{0,1,2,3\}$.

Так, для случая $k=2$ могут быть выписаны все аффинные функции в виде таблиц истинности

$$\begin{Bmatrix} 0000 & 0123 & 0202 & 0321 \\ 1111 & 1230 & 1313 & 1032 \\ 2222 & 2301 & 2020 & 2103 \\ 3333 & 3012 & 3131 & 3210 \end{Bmatrix}. \tag{7}$$

Вычеркивая из данного множества (7) все такие строки, которые являются линейной комбинацией, с точки зрения операции сложения со значениями 1, 2 или 3 по модулю 4, в результате останутся только четыре строки

$$\begin{array}{ll} \varphi_1=0; & \{0000\} \\ \varphi_5=x_1; & \{0123\} \\ \varphi_9=2x_1; & \{0202\} \\ \varphi_{13}=3x_1; & \{0321\} \end{array}. \tag{8}$$

Переходя к экспоненциальной системе счисления путем использования однозначного преобразования

$$\left\{e^{j\frac{2\pi}{4}\cdot0}\quad e^{j\frac{2\pi}{4}\cdot1}\quad e^{j\frac{2\pi}{4}\cdot2}\,e^{j\frac{2\pi}{4}\cdot3}\right\}\to\left\{e^{j0^\circ}\quad e^{j90^\circ}\quad e^{j180^\circ}\,e^{j270^\circ}\right\}\to\{z_0\quad z_1\quad z_2\quad z_3\}, \tag{9}$$

получаем матрицу Виленкина-Крестенсона

$$V_4 = \begin{bmatrix} z_0 & z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 & z_3 \\ z_0 & z_2 & z_0 & z_2 \\ z_0 & z_3 & z_2 & z_1 \end{bmatrix} = \begin{bmatrix} e^{j0^o} & e^{j0^o} & e^{j0^o} & e^{j0^o} \\ e^{j0^o} & e^{j90^o} & e^{j180^o} & e^{j270^o} \\ e^{j0^o} & e^{j180^o} & e^{j0^o} & e^{j180^o} \\ e^{j0^o} & e^{j270^o} & e^{j180^o} & e^{j90^o} \end{bmatrix}. \quad (10)$$

Отметим, что примененный ранее метод построения матриц Виленкина-Крестенсона является достаточно трудоемким, в то время, как метод [5] подразумевает поэлементный синтез таких матриц. Исследования позволили вывести формулу рекуррентного построения матриц Виленкина-Крестенсона любого заданного порядка $N = 4^k$

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \quad (11)$$

где «+» — операция сложения в соответствии с таблицей сложения (3), а матрицы V представлены в символической форме, т.е. суммирование выполняется относительно индексов z_i.

Например, запишем матрицу Виленкина-Крестенсона порядка $N = 16$

$$V_{16} = \begin{bmatrix} z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 & z_3 & z_0 & z_1 & z_2 & z_3 & z_0 & z_1 & z_2 & z_3 & z_0 & z_1 & z_2 & z_3 \\ z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 & z_0 & z_2 \\ z_0 & z_3 & z_2 & z_1 & z_0 & z_3 & z_2 & z_1 & z_0 & z_3 & z_2 & z_1 & z_0 & z_3 & z_2 & z_1 \\ z_0 & z_0 & z_0 & z_0 & z_1 & z_1 & z_1 & z_1 & z_2 & z_2 & z_2 & z_2 & z_3 & z_3 & z_3 & z_3 \\ z_0 & z_1 & z_2 & z_3 & z_1 & z_2 & z_3 & z_0 & z_2 & z_3 & z_0 & z_1 & z_3 & z_0 & z_1 & z_2 \\ z_0 & z_2 & z_0 & z_2 & z_1 & z_3 & z_1 & z_3 & z_2 & z_0 & z_2 & z_0 & z_3 & z_1 & z_3 & z_1 \\ z_0 & z_3 & z_2 & z_1 & z_1 & z_0 & z_3 & z_2 & z_2 & z_1 & z_0 & z_3 & z_3 & z_2 & z_1 & z_0 \\ z_0 & z_0 & z_0 & z_0 & z_2 & z_2 & z_2 & z_2 & z_0 & z_0 & z_0 & z_0 & z_2 & z_2 & z_2 & z_2 \\ z_0 & z_1 & z_2 & z_3 & z_2 & z_3 & z_0 & z_1 & z_0 & z_1 & z_2 & z_3 & z_2 & z_3 & z_0 & z_1 \\ z_0 & z_2 & z_0 & z_2 & z_2 & z_0 & z_2 & z_0 & z_0 & z_2 & z_0 & z_2 & z_2 & z_0 & z_2 & z_0 \\ z_0 & z_3 & z_2 & z_1 & z_2 & z_1 & z_0 & z_3 & z_0 & z_3 & z_2 & z_1 & z_2 & z_1 & z_0 & z_3 \\ z_0 & z_0 & z_0 & z_0 & z_3 & z_3 & z_3 & z_3 & z_2 & z_2 & z_2 & z_2 & z_1 & z_1 & z_1 & z_1 \\ z_0 & z_1 & z_2 & z_3 & z_3 & z_0 & z_1 & z_2 & z_2 & z_3 & z_0 & z_1 & z_1 & z_2 & z_3 & z_0 \\ z_0 & z_2 & z_0 & z_2 & z_3 & z_1 & z_3 & z_1 & z_2 & z_0 & z_2 & z_0 & z_1 & z_3 & z_1 & z_3 \\ z_0 & z_3 & z_2 & z_1 & z_3 & z_2 & z_1 & z_0 & z_2 & z_1 & z_0 & z_3 & z_1 & z_0 & z_3 & z_2 \end{bmatrix}. \quad (12)$$

Использование метрики Хэмминга или метрики Ли для сравнения расстояний нелинейности S-блоков, описанных с помощью многозначной логики, является непростой задачей, существенный прогресс в решении которой был достигнут в работе [8] за счет использования коэффициентов нелинейности. Изложим кратко суть данного метода применительно к 4-функциям.

Пусть, например, задана произвольная 4-функция длины $N = 16$ в виде своей таблицы истинности

$$A = \left\{ e^{j0} e^{j90} e^{j180} e^{j270} e^{j0} e^{j90} e^{j180} e^{j270} e^{j0} e^{j90} e^{j180} e^{j270} e^{j0} e^{j90} e^{j180} e^{j270} \right\}, \quad (13)$$

мы можем найти её коэффициенты преобразования Виленкина-Крестенсона

$$\Omega_A = A \cdot \overline{V}_{16} = \{0 \quad 16 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0\}. \quad (14)$$

Каждый коэффициент преобразования Виленкина-Крестенсона (14) характеризует степень содержания функции Виленкина-Крестенсона (строки матрицы V_N) в исследуемой последовательности.

Поскольку множество функций Виленкина-Крестенсона является множеством наиболее линейных функций, мы можем измерить степень линейности исследуемой функции с помощью максимального значения спектральных коэффициентов. Например, в нашем случае коэффициент линейности составляет $L = \max\left\{\left|\Omega_A\right|\right\} = 16$.

Полученный результат несложно объяснить, поскольку последовательность (13) является второй строкой матрицы Виленкина-Крестенсона (12), что привело к тому, что модуль второго значения спектрального коэффициента (14) принял максимально возможное значение, равное длине N.

Поскольку полный четверичный код может быть рассмотрен как линейное векторное пространство, в котором функции Виленкина-Крестенсона являются ортонормированным базисом, для преобразования Виленкина-Крестенсона справедливо равенство Парсеваля

$$\sum_{\omega=1}^{N}\left|\Omega(\omega)\right|^2 = 4^{2k}, \tag{15}$$

где k – число переменных, от которых зависит эквивалентная 4-функция, $k = \log_4 N$.

Минимальное же значение коэффициентов преобразования Виленкина-Крестенсона достигается тогда, когда их значения постоянны по модулю и равны

$$\left|\Omega_{\min}(\omega)\right| = \sqrt{\frac{4^{2k}}{4^k}} = 4^{k/2}, \quad \omega = 0,1,...,N-1. \tag{16}$$

Таким образом, нелинейность функций q-значной логики оценивается как разность между максимально возможным значением модуля коэффициента преобразования Виленкина-Крестенсона и максимальным значением (по модулю) преобразования Виленкина-Крестенсона исследуемой функции

$$NL = \begin{cases} q^k - \max\left\{\left|\Omega\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W\right|\right\}, & q = 2. \end{cases} \tag{17}$$

Выражение (17) является определением q-нелинейности S-блока. Рассмотрим один из S-блоков подстановки длины $N = 16$, используемый в криптоалгоритме Магма [9]:

$$S = [6 \quad 8 \quad 2 \quad 3 \quad 9 \quad 10 \quad 5 \quad 12 \quad 1 \quad 14 \quad 4 \quad 7 \quad 11 \quad 13 \quad 0 \quad 15]. \tag{18}$$

Представляя данный S-блок в виде компонентных булевых функций

$$F_2 = \begin{bmatrix} 0100110101001101 \\ 1000001101110101 \\ 1011010001011001 \\ 0001101010011101 \end{bmatrix}, \tag{19}$$

нетрудно найти, что его 2-нелинейность равна $N2_S = \min\{4,4,4,4\} = 4$.

Тем не менее, этот же S-блок возможно представить в виде компонентных 4-функций

$$F_4 = \begin{bmatrix} 1200221313112303 \\ 2023121012033103 \end{bmatrix}, \quad (20)$$

для каждой из которых найдем абсолютные значения спектральных коэффициентов Виленкина-Крестенсона

$$|\Omega| = \begin{bmatrix} 0 & 4{,}472 & 6{,}325 & 4{,}472 & 2{,}828 & 2 & 0 & 6 & 5{,}657 & 2 & 2{,}828 & 6 & 2{,}828 & 6 & 0 & 2 \\ 0 & 2{,}828 & 4 & 6{,}325 & 2 & 4{,}472 & 2 & 2 & 2{,}828 & 0 & 2{,}828 & 4 & 4{,}472 & 4{,}472 & 8{,}246 & 4{,}472 \end{bmatrix}. \quad (21)$$

Применяя формулу (17), а также методику оценки нелинейности S-блоков [8], находим, что 4-нелинейность равна

$$N4_S = \min\{NL\} = \min\{9{,}675,\ 7{,}754\} = 7{,}754\,. \quad (22)$$

В табл. 1 представлены расчеты двоичной ($N2_S$) и четверичной ($N4_S$) нелинейности для S-блоков подстановки длины $N = 16$ различных конструкций.

Таблица 1 – Двоичное и четверичное расстояние нелинейности некоторых S-блоков

Вид S-блока	S-блоки «Магма» [9]	Конструкция Ниберг над $GF(2^4)$ [10]	Двоичные последовательности де Брейна [11]	Четверичные последовательности де Брейна [12]
$N2_S$	4	4	1…4	0…4
$N4_S$	7,056…9,675	7,5147…9,675	4,955…9,675	5,2297…10,3431

Исследование данных табл. 1 показывает, что S-блоки шифра «Магма» [9], конструкции Ниберг, а также S-блоки на основе двоичных последовательностей де Брейна не всегда обладают высокой 4-нелинейностью, т.е. часто довольно легко аппроксимируются четверичными аффинными функциями.

В этом свете, актуальной видится задача разработки методов синтеза S-блоков подстановки с заданным уровнем 4-нелинейности.

Метод синтеза сильно нелинейных подстановок длины $N = 16$. Метод синтеза S-блоков подстановки, обладающих максимальной нелинейностью (как 2-нелинейностью, так и 4-нелинейностью) основан на следующем подходе: сначала на основе высоконелинейных булевых функций синтезируются 4-функции, обладающие максимально возможной 4-нелинейностью, после чего на их основе производится синтез S-блоков.

Предлагаемый метод синтеза S-блоков подстановки, обладающих максимальной нелинейностью, изложим в виде шагов, сопровождаемых конкретными примерами.

Шаг 1. Построить множество максимально нелинейных 4-функций.

Отметим, что поиск максимально нелинейных 4-функций сопряжен с перебором множества мощности $J_4^{16} = 4^{16} = 2^{32}$, что затруднено с вычислительной точки зрения. Мы предлагаем следующий алгоритм для синтеза максимально нелинейных 4-функций на основе максимально нелинейных булевых функций.

Шаг 1.1. Перебрав полное множество булевых функций длины $N = 16$, мощности $J_2^{16} = 2^{16} = 65536$ отберем из них такие, которые являются сбалансированными и при этом

обладают наибольшей 2-нелинейностью $N_f = 4$. Всего таких булевых функций существует $J_{Nf4} = 10920$ штук.

Шаг 1.2. Производим конкатенацию найденных нелинейных булевых функций в 4-функцию и измеряем её 4-нелинейность в соответствии с (17).

Например, пусть выбраны следующие 2 булевы функции из множества булевых функций, построенных на *Шаге 1.1*, на основе которых нетрудно построить новую 4-функцию f_1

$$\begin{array}{lcccccccccccccccc} g_1 = & \{ & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \}; \\ g_2 = & \{ & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \}; \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \}. \end{array} \quad (23)$$

Исследования показывают следующее распределение 4-нелинейностей в синтезированном классе из 10920^2 4-функций.

Таблица 2 – Распределение 4-нелинейностей в синтезированном классе 4-функций

4-нелинейность	3,3509	4	4,6863	5,2297	5,8020	6	7,0557	7,5147
Количество 4-функций	7168	53376	120832	387072	979968	1831936	6745472	7279104
4-нелинейность	7,7538	8	8,7889	9,6754	10	10,3431	11,5279	–
Количество 4-функций	12682240	12472448	27601920	42826240	3834880	2417600	6144	–

Оказывается, что среди множества 4-функций с 4-нелинейностью 11,5279 не существует сбалансированных 4-функций. Таким образом, максимальное значение 4-нелинейности, которым могут обладать S -блоки с 2-нелинейностью $N_f = 4$, равно 10,3431.

Шаг 2. Выбрать заданную компонентную 4-функцию и достроить к ней пару так, чтобы они составляли биективный S-блок подстановки.

Например, рассмотрим 4-функцию

$$\begin{array}{lcccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \} \\ f_2 = & \{ & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * & \}. \end{array} \quad (24)$$

В позициях, в которых функция $f_1 = 0$, 4-функция f_2 должна принимать 4 различных значения из множества $\{0,1,2,3\}$ для того, чтобы S-блок был биективным. Всего различных комбинаций, соответственно, может быть $4! = 24$. Расставим один из возможных наборов функции f_2 в тех позициях, где $f_1 = 0$

$$\begin{array}{lcccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \} \\ f_2 = & \{ & * & * & * & * & * & * & * & 0 & * & * & * & * & * & 1 & 2 & 3 & \}. \end{array} \quad (25)$$

Аналогичным образом выбираем один из $4! = 24$ наборов для функции f_2 на позициях, где $f_1 = 1,2,3$. В результате, например, получаем следующую пару 4-функций, определяющую S-блок

$$\begin{array}{lcccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\ f_1 = & \{ & 3 & 3 & 1 & 1 & 3 & 1 & 2 & 0 & 3 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & \} \\ f_2 = & \{ & 0 & 1 & 0 & 1 & 3 & 2 & 1 & 0 & 2 & 3 & 2 & 3 & 0 & 1 & 2 & 3 & \} \\ S = & \{ & 3 & 7 & 1 & 5 & 15 & 9 & 6 & 0 & 11 & 13 & 10 & 14 & 2 & 4 & 8 & 12 & \}. \end{array} \quad (26)$$

Шаг 3. Отсеиваем все такие S-блоки, вторая компонентная 4-функция которых не обладает 4-нелинейностью 10,3431.

Для нашего примера, задав 4-функцию f_1 (24), мы можем построить 5225 S-блоков, обладающих 4-нелинейностью 10,3431.

Выводы:

1. Предложена методика оценки 4-нелинейности функций многозначной логики на основе преобразования Виленкина-Крестенсона, отражающая степень равномерности спектра Виленкина-Крестенсона (содержания в компонентных 4-функциях S-блока подстановки четверичных аффинных функций).

2. Проведено исследование нелинейных свойств S-блоков современных криптографических алгоритмов с помощью предложенной методики оценки 4-нелинейности, которое показало, что они не всегда являются стабильными даже для конструкции Ниберг, используемой в американском стандарте шифрования AES/Rijndael. Данное обстоятельство диктует необходимость разработки методов синтеза S-блоков подстановки, обладающих высоким уровнем 4-нелинейности.

3. Предложен конструктивный метод синтеза S-блоков длины $N=16$, обладающих высоким уровнем 4-нелинейности на основе заданных высоконелинейных булевых функций. Построенные S-блоки могут быть рекомендованы к практическому применению в действующих криптоалгоритмах.

Актуальной видится задача дальнейшего совершенствования предложенного метода синтеза 4-нелинейных S-блоков, в частности, для построения S-блоков больших длин, например, длины $N=256$, используемой в криптоалгоритме AES/Rijndael. Решение этой задачи является предметом дальнейших исследований.

ЛИТЕРАТУРА:

1. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Прикладная дискретная математика, 2009. – № 1(3). – С. 15–37.
2. Соколов А.В. Новые методы синтеза нелинейных преобразований современных шифров / А.В. Соколов. – Lap Lambert Academic Publishing, Germany, 2015. – 100 с.
3. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М: Издательство МЦНМО, 2004. – 472 с.
4. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков // Наука и Техника. – 2010. – С. 340.
5. Трахтман А.М. Основы теории дискретных сигналов на конечных интервалах / А.М. Трахтман, В.А. Трахтман. – М.: Сов.радио, 1975. — 208 с.
6. Жданов О.Н. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен / О.Н. Жданов, А.В. Соколов // Проблемы физики, математики и техники. – 2015. – № 3(24). – С. 94–97.
7. Соколов А.В. Генератор псевдослучайных ключевых последовательностей на основе тройственных наборов бент-функций / А.В. Соколов, О.Н. Жданов, Н.А. Барабанов // Проблемы физики, математики и техники. – 2016. – № 1 (26). – С. 85–91.
8. Sokolov A.V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A.V. Sokolov, O. N. Zhdanov // Journal of Telecommunication, Electronic and Computer Engineering. – VOL 8. – NO 9. – P. 39–43.
9. Национальный стандарт Российской Федерации. Информационные технологии. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12. – М.: Стандартинформ, 2015. – 25 с.
10. Мазурков М.И. Криптографические свойства нелинейного преобразования шифра RIJNDAEL на базе полных классов неприводимых полиномов / М.И. Мазурков, А.В. Соколов // Праці Одеського політехнічного університету. – 2012. – Вип. 2 (39). – С.183–189.
11. Мазурков М.И. Методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения / М.И. Мазурков, А.В. Соколов // Труды ОНПУ. – 2012. – Вип. 1(38). – С.188–198.

12. Мазурков М.И. Конструктивный метод синтеза полных классов многоуровневых последовательностей де Брейна / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2013. – Т. 56. – N 1. – С. 43–49.

REFERENCES:

1. Tokareva N.N. Bent-functions: results and applications. Review of works / N.N. Tokareva // PDM. – 2009. – № 1 (3), 15–37.
2. Sokolov A.V. New methods of synthesis of nonlinear transform of modern ciphers / A.V. Sokolov. – Lap Lambert Academic Publishing, Germany, 2015. – 100 p.
3. Logachev O.A. Boolean functions in the theory of coding and cryptology / O.A. Logachev, A.A. Salnikov, V.V. Yashchenko. – M: MKNMO Publishing House. – 2004. – 472 p.
4. Mazurkov M.I. Broadband radio telecommunication systems / M.I. Mazurkov // Science and Technology. – 2010. – P. 340.
5. Trachtman A.M. Fundamentals of the theory of discrete signals on finite intervals / A.M. Trakhtman, V.A. Trachtman. – Moscow: Sov. radio, 1975. – 208 p.
6. Zhdanov O.N. Algorithm of construction of optimal according to criterion of zero correlation nonbinary S-boxes / O.N. Zhdanov, A.V. Sokolov // Problems of Physics, Mathematics and Technics. – 2015. – No. 3 (24). – P. 94–97.
7. Sokolov A.V. Pseudo-random key sequence generator based on triple sets of bent-functions / A.V. Sokolov, O.N. Zhdanov N.A. Barabanov // Problems of Physics, Mathematics and Technics. – 2016. – No. 1 (26). – P. 85–91.
8. Sokolov A.V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A.V. Sokolov, O. N. Zhdanov // Journal of Telecommunication, Electronic and Computer Engineering. – Vol. 8. – No 9. – P. 39–43.
9. The national standard of the Russian Federation. Information Technology. Cryptographic protection of information. Block ciphers. GOST R 34.12. 2015. – M.: Standartinform, 2015. – 25 p.
10. Mazurkov M.I. Cryptographic properties of the nonlinear transform of the RIJNDAEL cipher on the basis of complete classes of irreducible polynomials / M.I. Mazurkov, A.V. Sokolov // Proceedings of the Odessa Polytechnic University. – 2012. – Series 2 (39). – P.183–189.
11. Mazurkov M.I. Synthesis methods of pseudo-random binary sequences with the property of the k-gram distribution for encryption tasks / M.I. Mazurkov, A.V. Sokolov // Proceedings of ONPU. – 2012. – No. 1(38). – P.188–198.
12. Mazurkov M.I. Constructive method for synthesis of complete classes of multilevel de Bruijn sequences / M.I. Mazurkov, A.V. Sokolov // Proceedings of Universities. Radioelectronics. – 2013. – Vol. 56. – No 1. – P. 43–49.