МЕТОДИКА ОЦЕНКИ НЕЛИНЕЙНОСТИ S-БЛОКОВ НА ОСНОВЕ ЧЕТВЕРИЧНОГО ПРЕОБРАЗОВАНИЯ ВИЛЕНКИНА–КРЕСТЕНСОНА

Н. И. Красота, к. т. н. А. В. Соколов

Одесский национальный политехнический университет
Украина, г. Одесса
radiosquid@gmail.com

Разработана методика оценки нелинейности S-блоков на основе четверичного преобразования Виленкина–Крестенсона. Введено определение четверичной нелинейности, проведено исследование четверичной нелинейности S-блоков на основе двоичных и четверичных последовательностей де Брейна, S-блоков конструкции Ниберг, а также набора подстановочных конструкций шифра «Магма». Предложенный критерий является основой для дальнейшего совершенствования существующих подстановочных конструкций.

Ключевые слова: S-блок подстановки, преобразование Виленкина–Крестенсона, нелинейность.

Нелинейные *S*-блоки являются основным элементом блочных симметричных шифров [1], к которым предъявляются строгие критерии качества. Одним из таких критериев является нелинейность *S*-блока, измеряемая как расстояние Хэмминга до множества двоичных аффинных функций [1]. Тем не менее, при атаке на алгоритм шифрования криптоаналитик не стеснен в используемых средствах и может использовать аппроксимацию элементов шифра методами многозначной логики. Таким образом, для более полного исследования нелинейных свойств *S*-блоков имеет смысл оценивать их нелинейность не только в терминах двоичной логики, но и с учетом принципов многозначной логики.

Целью настоящей работы является разработка методики исследования нелинейных свойств *S*-блоков подстановки на основе четверичного преобразования Виленкина–Крестенсона.

Матрицы Виленкина–Крестенсона являются обобщением матриц Адамара на многозначный случай. Классический подход к определению матриц Виленкина–Крестенсона изложен в [2], тогда как проведенные исследования позволили вывести формулу рекуррентного построения матриц Виленкина–Крестенсона любого заданного порядка $N = 4^k$, $k = 1, 2, ...$:

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \end{bmatrix}, \; V_1 = 0 . \qquad (1)$$

где «+» — операция сложения mod4, а матрицы V представлены в символической форме, т. е. соответствуют однозначному преобразованию алфавита

$$A = \{e^{j(2\pi/4)\cdot 0} \quad e^{j(2\pi/4)\cdot 1} \quad e^{j(2\pi/4)\cdot 2} \; e^{j(2\pi/4\cdot)3}\} \leftrightarrow \{e^{j0^\circ} \quad e^{j90^\circ} \quad e^{j180^\circ} \; e^{j270^\circ}\} \leftrightarrow \{0,1,2,3\} . \qquad (2)$$

Спектральные коэффициенты $W(w)$ дискретной последовательности находятся путем умножения вектора-столбца, содержащего отсчёты сигнала на комплексно сопряженную матрицу преобразования $\overline{V}$. Методика определения нелинейности компонентных 4-функций *S*-блоков подстановки основана на троичной методике [3] и подразумевает следующее: каждый спектральный коэффициент Виленкина–Крестенсона характеризует степень содержания функции Виленкина–Крестенсона в исследуемой последовательности.

В [3] было выведено следующее соотношение для определения нелинейности функций *q*-значной логики, которая оценивается как разность между максимально возможным значением модуля коэффициента преобразования Велинкина–Крестенсона и максимальным значением (по модулю) преобразования Виленкина–Крестенсона исследуемой функции

$$Nq_S = q^k - \max\{|W|\}, q > 2 . \qquad (3)$$

Рассмотрим первый высоконелинейный S-блок подстановки криптоалгоритма «Магма» [4]

$$S = [12 \quad 4 \quad 6 \quad 2 \quad 10 \quad 5 \quad 11 \quad 9 \quad 14 \quad 8 \quad 13 \quad 7 \quad 0 \quad 3 \quad 15 \quad 1]. \qquad (4)$$

Представляя данный *S*-блок в виде компонентных булевых функций нетрудно найти, что его расстояние нелинейности равно $N2_S = \min\{4, 4, 4, 4\} = 4$.

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

$$F_4 = \begin{bmatrix} 0 & 0 & 2 & 2 & 2 & 1 & 3 & 1 & 2 & 0 & 1 & 3 & 0 & 3 & 3 & 1 \\ 3 & 1 & 1 & 0 & 2 & 1 & 2 & 2 & 3 & 2 & 3 & 1 & 0 & 0 & 3 & 0 \end{bmatrix}. \qquad (5)$$

Находя модули спектральных коэффициентов Виленкина–Крестенсона, видим, что каждая из компонентных 4-функций обладает разным максимальным значением модуля спектрального коэффициента, т. е. разным содержанием в себе той или иной аффинной 4-функции. Таким образом, с точки зрения 4-логики, расстояния нелинейности данных компонентных функций являются различными.

Применяя формулу (3) находим, что четверичное расстояние нелинейности *S*-блока (4) равно $N4_S = \min\{NL\} = \min\{8.788, 7.055\} = 7.055$.

В таблице представлены результаты расчета двоичного и четверичного расстояния нелинейности для *S*-блоков подстановки длины $N = 16$ различных конструкций.

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

Анализ приведенных в таблице данных показывает, что *S*-блоки шифра «Магма», конструкции Ниберг, а также *S*-блоки на основе двоичных последовательностей де Брейна не всегда обладают высоким четверичным расстоянием нелинейности, т. е. довольно легко аппроксимируются четверичными аффинными функциями. С точки зрения равномерности спектра Виленкина–Крестенсона наилучшие результаты показывают *S*-блоки на основе четверичных последовательностей де Брейна, например

$$S = \{14 \quad 9 \quad 7 \quad 15 \quad 13 \quad 5 \quad 6 \quad 10 \quad 8 \quad 2 \quad 11 \quad 12 \quad 1 \quad 4 \quad 0 \quad 3\}, \qquad (6)$$

для которого $N2_S = 4$ и $N4_S = 10{,}343$.

Таким образом, предложена методика исследования нелинейных свойств *S*-блоков подстановки на основе четверичного преобразования Виленкина–Крестенсона, отражающая степень равномерности спектра Виленкина–Крестенсона (содержания в компонентных 4-функциях *S*-блока подстановки четверичных аффинных функций). Исследованы нелинейные свойства некоторых классов *S*-блоков подстановки, которые показали нестабильность данного показателя.

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

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Соколов, А.В. Новые методы синтеза нелинейных преобразований современных шифров.— Lap Lambert Academic Publishing, Germany 2015.

2. Трахтман А.М., Трахтман В.А. Основы теории дискретных сигналов на конечных интервалах.— Москва: Сов. радио, 1975.

3. Sokolov A.V., Zhdanov O. N. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties.— JTEC. — Vol. 8. — N 9. — P. 39—43.

———————

N. I. Krasota, A. V. Sokolov

An S-box nonlinearity estimation method based on a quaternary Vilenkin-Christenson transform

This paper is devoted to the development of an S-box nonlinearity estimation method based on the quaternary Vilenkin-Christenson transform. We introduced the definition of a quaternary nonlinearity and performed the research of quaternary non-linearity of S-boxes based on binary and quaternary de Brain sequences, Nyberg construction S-boxes, as well as a set of «Magma» cipher S-boxes. The proposed criterion is the basis for further improvement of existing nonlinear substitution constructions.

Keywords: S-box, Vilenkin-Christenson transform, nonlinearity.