О. Н. Жданов, А. В. Соколов, Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен, *ПФМТ*, 2015, выпуск 3(24), 94–97

ИНФОРМАТИКА

УДК 004.056.55

АЛГОРИТМ ПОСТРОЕНИЯ ОПТИМАЛЬНЫХ ПО КРИТЕРИЮ НУЛЕВОЙ КОРРЕЛЯЦИИ НЕДВОИЧНЫХ БЛОКОВ ЗАМЕН

О.Н. Жданов[1], **А.В. Соколов**[2]

[1]*Сибирский государственный аэрокосмический университет им. академика М.Ф. Решетнёва*, *Красноярск*, *Россия*
[2]*Одесский национальный политехнический университет*, *Одесса*, *Украина*

ALGORITHM OF CONSTRUCTION OF OPTIMAL ACCORDING TO CRITERION OF ZERO CORRELATION NON-BINARY *S*-BOXES

O.N. Zhdanov[1], **A.V. Sokolov**[2]

[1]*M.F. Reshetnev Siberian State Aerospace University*, *Krasnoyarsk*, *Russia*
[2]*Odessa National Polytechnic University*, *Odessa*, *Ukraine*

Рассматриваются вопросы построения криптографических *S*-блоков подстановки длины $N = 3^k$, оптимальных с точки зрения отсутствия корреляции между векторами выхода и входа. Построенные множества *S*-блоков подстановки могут быть рекомендованы для модернизации существующих блочных симметричных шифров, а также для конструирования новых быстродействующих алгоритмов шифрования, основанных на принципах многозначной логики.

Ключевые слова*: S-блок подстановки*, *матрица коэффициентов корреляции*, *схема Кима.*

This paper considers the construction of cryptographic *S*-boxes of the length $N = 3^k$, which are optimal from the point of view of the absence of correlation between the output and input vectors. Constructed sets of *S*-boxes can be recommended for upgrading of the existing block symmetric ciphers, as well as for the synthesis of new high-speed encryption algorithms based on the principles of multi-valued logic.

Keywords: *S-box*, *matrix of correlation coefficients*, *Kim scheme.*

Введение

Важнейшим компонентом современных блочных симметричных криптографических алгоритмов является *S*-блок подстановки, который представляет собой отображение множества входных битов во множество выходных битов. Данная конструкция во многом определяет криптостойкость и быстродействие блочных симметричных шифров, в которых она применяется.

К качеству *S*-блоков подстановки предъявляются определенные требования, в частности, низкая корреляционная связь векторов выхода и входа *S*-блока подстановки. Оптимальной является ситуация, когда каждый бит выходного блока статистически независим от каждого бита входного блока.

Считающийся стойким и являющийся одним из наиболее популярных в настоящее время алгоритм Rijndael [1] полностью определяет блок замен заданием неприводимого полинома над полем Галуа. Однако, будучи не единственно возможным (и не по всем параметрам оптимальным) для построения шифра, этот полином предлагается для применения всем пользователям, что не является бесспорным достоинством. Примером другого подхода служит алгоритм ГОСТ 28147-89 [2], в котором каждый пользователь применяет свои, уникальные блоки замен, но алгоритм не определяет способ их построения. Из сказанного ясно, что для получения криптосистемы высокой надежности следует попытаться соединить достоинства обоих подходов, а именно: разработать такую методику, которая позволит получать большое количество высококачественных *S*-блоков каждому пользователю.

В статье мы рассматриваем последовательности входных и выходных битов как значения случайных величин и ставим себе задачу получение блока замен с нулевыми коэффициентами корреляции выходных и входных битовых последовательностей. Более формально: мы добиваемся того, что коэффициент корреляции векторов выхода y_μ и входа x_ν равен $r_{\nu,\mu} = 0$.

Работы [3], [4] посвящены построению корреляционно-иммунных *S*-блоков подстановки длины $N = 2^k$, соответствующих критерию нулевой корреляции между векторами выхода и входа.

Тем не менее, бурное развитие современных вычислительных устройств, а также активное внедрение *m*-ичных систем передачи и обработки информации [5] диктует необходимость разработки методов синтеза криптографически качественных *S*-блоков подстановки других длин *N*, например, $N = 3^k$.

Целью настоящей статьи является разработка алгоритма синтеза бесконечных семейств S-блоков подстановки соответствующих критерию нулевой корреляции векторов выхода и входа длин $N = 3^k$, $k = 2,3,4...$

1 Методика вычисления матрицы коэффициентов корреляции

***Определение* 1.1.** *Матрицей коэффициентов корреляции S-блока длины* $N = p^k$ *назовем матрицу* $\mathrm{P} = \left\| \rho_{\nu,\mu} \right\|$, $\nu,\mu = \overline{1,k}$, *элементы которой вычисляются в соответствии с формулой* [6, с. 425]:

$$\rho_{\nu,\mu} = \frac{\sum\limits_{t=1}^{N} x_{\nu,t} y_{\mu,t} - \dfrac{\sum\limits_{t=1}^{N} x_{\nu,t} \sum\limits_{t=1}^{N} y_{\mu,t}}{N}}{\sqrt{\left[\sum\limits_{t=1}^{N} x_{\nu,t}^2 - \dfrac{\left(\sum\limits_{t=1}^{N} x_{\nu,t}\right)^2}{N}\right] \cdot \left[\sum\limits_{t=1}^{N} y_{\mu,t}^2 - \dfrac{\left(\sum\limits_{t=1}^{N} y_{\mu,t}\right)^2}{N}\right]}}, \quad (1.1)$$

$$\nu, \mu = 1,2,...,k,$$

где μ, ν – номера компонентных булевых функций исследуемого *S*-блока и тривиальной подстановки 0, 1,…, *N*–1 соответственно, $k = \log_p N$ – количество компонентных булевых функций.

Замечание. В случае, когда $\{x_\nu\}$ и $\{y_\mu\}$ – двоичные векторы, можно пользоваться частным случаем формулы (1.1) [3]:

$$r_{\nu,\mu} = 1 - 2^{-(k-1)} \sum_{t=1}^{N} \left(x_{\nu,t} \oplus y_{\mu,t} \right) = 0, \quad (1.2)$$

$$\nu, \mu = \overline{1,k}.$$

***Определение* 1.2.** *Нелинейное преобразование называется оптимальным, если все его коэффициенты корреляции равны нулю*

$$\rho_{\nu,\mu} = 0, \ \forall \nu,\mu = 1,2,...,k.$$

2 Алгоритм синтеза оптимальных S-блоков

На наш взгляд, удачной является идея двухэтапного построения блоков [3]. На первом этапе генерируем блок замен небольшой длины, например, длины $N = 9$. Оптимальные *S*-блоки замен для данной длины могут быть легко найдены переборным методом. На втором этапе предлагается использование схемы Кима [5], которая позволяет из построенных небольших *S*-блоков получить блоки нужной длины при сохранении их оптимальности. Схема Кима в общем виде представлена на рисунке 2.1.

Пример. Рассмотрим последовательность, представляющую собой *S*-блок подстановки длины $N = 3^2 = 9$

$$S_9 = \begin{Bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 2 & 6 & 8 & 7 & 5 & 4 & 3 & 1 \end{Bmatrix}. \quad (2.1)$$

Вычисляя его матрицу коэффициентов корреляции в соответствии с (1.1), получаем

$$\mathrm{P} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Применим к блоку (2.1) схему рекуррентного увеличения длины (рисунок 2.1), которая, учитывая длину исходного *S*-блока $N = 9$ и длину требуемого *S*-блока $N = 27$ принимает вид (рисунок 2.2).

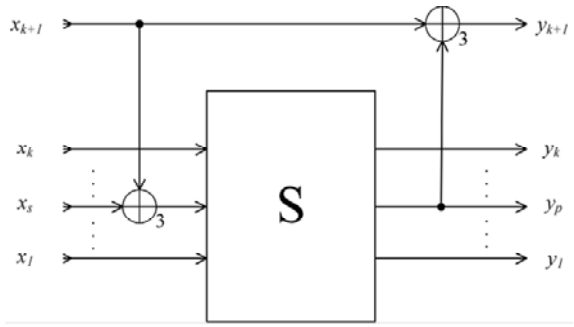

Рисунок 2.1 – Схема Кима

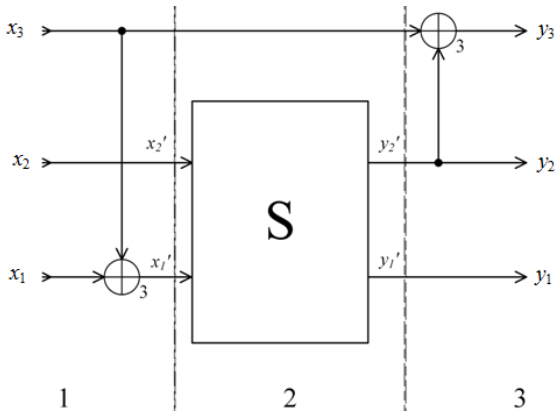

Рисунок 2.2 – Схема Кима для *S*-блока с двумя входами

Пример работы схемы Кима рассмотрим с помощью вычисления выходных значений на конкретных итерациях:

Значение нового S-блока на итерации 0. Пусть на вход схемы (рисунок 2.2) поступило сочетание исходных данных $X = (x_1, x_2, x_3)$

$$x_1 = 0, \ x_2 = 0, \ x_3 = 0 \Rightarrow X = 0,$$

тогда, вычисляя сумму в первом подблоке вычислений, получаем

$$x_1' = x_1 + x_3 = 0 + 0 = 0, \ x_2' = 0,$$

после преобразования, во втором подблоке

$$S_9(0,0) = S_9(0) = 0, \ y_1' = 0, y_2' = 0.$$

и наконец, вычисления в третьем подблоке схемы:

$$y_1 = y_1' = 0, \ y_2 = y_2' = 0,$$

$$y_3 = x_3 + y_2' = 0 + 0 = 0 \Rightarrow S_{27}(0) = 0.$$

Покажем вычисление значения нового S-блока на еще одной итерации, например, на итерации 19. Пусть на вход схемы (рисунок 2.2) поступило сочетание исходных данных $X = (x_1, x_2, x_3)$

$$x_1 = 1,\ x_2 = 0,\ x_3 = 2 \Rightarrow X = 19,$$

тогда, вычисляя сумму в первом подблоке вычислений получаем

$$x_1' = x_1 + x_3 = 1 + 2 = 0,\ \ x_2' = 0,$$

после преобразования, во втором подблоке

$$S_9(0,0) = S_9(0) = 0,$$

$$y_1' = 0,\ y_2' = 0.$$

И наконец, вычисления в третьем подблоке схемы:

$$y_1 = y_1' = 0,\ \ y_2 = y_2' = 0,$$

$$y_3 = x_3 + y_2' = 2 + 0 = 2 \ \Rightarrow\ S_{27}(19) = 18.$$

Таким образом, проводя все итерации, в итоге получаем требуемый *S*-блок подстановки S_{27} длины $N = 27$:

$$S_{27} = \left\{ \begin{array}{c} 0, 2, 24, 26, 25, 14, 13, 12, \\ 1, 9, 11, 6, 8, 7, 23, 22, 21, 10, \\ 18, 20, 15, 17, 16, 5, 4, 3, 19 \end{array} \right\}.$$

По формуле (1.1) получаем матрицу коэффициентов корреляции данного блока

$$R = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

что подтверждает соответствие *S*-блока определению 1.2.

Данные проведенных вычислительных экспериментов позволили установить, что в полном множестве *S*-блоков подстановки длины $N = 9$, мощность которого 9!=362880, существует подмножество из $|\Omega| = 264$ оптимальных *S*-блоков подстановки. Непосредственными вычислениями нами установлено, что свойство оптимальности является инвариантным по отношению к операции перестановки столбцов *S*-блока в обратном порядке.

Таким образом, приведем алгоритм синтеза *S*-блоков подстановки, оптимальных по критерию нулевой корреляции между векторами выхода и входа.

Шаг 1. Методом перебора найти все *S*-блоки малой длины, соответствующие критерию нулевой корреляции между векторами выхода и входа.

Шаг 2. Применяя схему Кима (рисунок 2.1) увеличить длину *S*-блока в 3 раза. Отметим, что при этом соединения в схеме Кима могут быть выполнены k^2 различными способами.

Шаг 3. Производим размножение полученного множества *S*-блоков подстановки, основываясь на сохранении оптимальности, при перестановке столбцов в обратном порядке. Таким образом, мощность нового множества будет $J_{3^{k+1}} = 2k^2 J_{3^k}$.

Шаг 4. Если достигнута требуемая длина *S*-блока, завершаем работу алгоритма, иначе переходим к Шагу 2.

3 Результаты вычислительных экспериментов

Применяя рекуррентное увеличение длины, легко получить оптимальные блоки любой длины вида $N = 3^k$. Отметим, что используя полное множество из $|\Omega_9| = 264$ *S*-блоков длины $N = 9$, разработанным методом мы можем получить $2 \cdot 4 \cdot 264 = 2112$ *S*-блоков длины $N = 27$, $2 \cdot 9 \cdot 2112 = 38016$ *S*-блоков длины $N = 81$, $2 \cdot 16 \cdot 38016 = 1216512$ *S*-блоков длины $N = 243$ и т. д.

Например, после троекратного проведения этой операции получим из исходного блока следующий, также являющийся оптимальным:

$$S_{243} = \left\{ \begin{array}{c} 0, 81, 162, 80, 161, 242, 12, 93, 174, 230, \\ 68, 149, 218, 56, 137, 214, 52, 133, 105, \\ 186, 24, 121, 202, 40, 109, 190, 28, 3, \\ 84, 165, 74, 155, 236, 15, 96, 177, 233, 71, \\ 152, 221, 59, 140, 208, 46, 127, 99, 180, \\ 18, 124, 205, 43, 112, 193, 31, 6, 87, 168, \\ 77, 158, 239, 9, 90, 171, 227, 65, 146, 224, \\ 62, 143, 211, 49, 130, 102, 183, 21, 118, \\ 199, 37, 115, 196, 34, 1, 82, 163, 78, 159, \\ 240, 13, 94, 175, 228, 66, 147, 216, 54, \\ 135, 215, 53, 134, 106, 187, 25, 122, 203, \\ 41, 110, 191, 29, 4, 85, 166, 72, 153, 234, \\ 16, 97, 178, 231, 69, 150, 219, 57, 138, \\ 209, 47, 128, 100, 181, 19, 125, 206, 44, \\ 113, 194, 32, 7, 88, 169, 75, 156, 237, 10, \\ 91, 172, 225, 63, 144, 222, 60, 141, 212, \\ 50, 131, 103, 184, 22, 119, 200, 38, 116, \\ 197, 35, 2, 83, 164, 79, 160, 241, 14, 95, \\ 176, 229, 67, 148, 217, 55, 136, 213, 51, \\ 132, 107, 188, 26, 120, 201, 39, 108, 189, \\ 27, 5, 86, 167, 73, 154, 235, 17, 98, 179, \\ 232, 70, 151, 220, 58, 139, 207, 45, 126, \\ 101, 182, 20, 123, 204, 42, 111, 192, 30, \\ 8, 89, 170, 76, 157, 238, 11, 92, 173, 226, \\ 64, 145, 223, 61, 142, 210, 48, 129, 104, \\ 185, 23, 117, 198, 36, 114, 195, 33 \end{array} \right\}.$$

Следующая итерация позволит получить блок размером 3^6=729.

Мы можем работать с любым представлением блока: в виде десятичного числа или в виде троичного, а после выполнения замен переход (при необходимости) к двоичному (битовому) формату не вызывает затруднений. Получив множество блоков замен с нулевыми коэффициентами корреляции выходных и входных битов, можно выбрать из них блоки с максимально возможной нелинейностью [3], [4], [7], [8].

Замечание 3.1. Проведенные рассуждения и вычисления с достаточно очевидными изменениями можно провести для любого простого p. При этом чем больше p, тем меньшее количество итераций требуется для построения блоков сравнимой длины.

Так, например, для построения семейства S-блоков подстановки длины $N = 5^k$ может быть использован первоначальный оптимальный S-блок

$$S_{25} = \begin{Bmatrix} 15, 8, 6, 17, 13, 24, 5, 20, \\ 4, 18, 3, 11, 9, 22, 2, 1, 7, \\ 21, 6, 12, 14, 23, 10, 19, 0 \end{Bmatrix}.$$

Замечание 3.2. Представляет интерес получение достаточных (и легко проверяемых) условий оптимальности блока, что позволит отказаться от метода перебора при их построении.

Выводы

Дальнейшее развитие получил алгоритм Кима рекуррентного увеличения длины S-блоков подстановки, в рамках чего разработан метод построения S-блоков подстановки оптимальных по критерию нулевой корреляции векторов выхода и входа длины $N = 3^k$.

Результаты вычислительных экспериментов подтверждают эффективность разработанного алгоритма для построения больших S-блоков подстановки, в частности, построен S-блок подстановки длины $N = 3^5 = 243$.

Построенные S-блоки подстановки могут быть использованы для модификации существующих и построения новых алгоритмов блочного симметричного шифрования.

ЛИТЕРАТУРА

1. *FIPS* 197 [Electronic resource]: Advanced encryption standard. – 2001. – Mode of access: http://csrc.nist.gov/publications/. – Date of access: 03.03.2015.

2. *Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования*: ГОСТ 28147-89. – М.: ИПК Издательство стандартов, 1996. – 28 с.

3. *Мазурков*, *М.И.* Метод синтеза оптимальных подстановочных конструкций по критерию нулевой корреляции между выходными и входными векторами данных / М.И. Мазурков // Известия высших учебных заведений. Радиоэлектроника. – 2012. – Т. 55, № 12. – С. 12–22.

4. *Мазурков*, *М.И.* Метод синтеза S-блоков по критерию нулевой корреляции между выходными и входными векторами данных и строгому лавинному критерию / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2014. – Т. 57, № 8. – С. 54–60.

5. *Kim*, *K.* Construction of DES-like *S*-boxes Based on Boolean Functions Satisfying the SAC / K. Kim. – Proc. of Asiacrypt'91, Springer Verlag. – 1991. – P. 59–72.

6. *Кремер*, *Н.Ш.* Теория вероятностей и математическая статистика / Н.Ш. Кремер. – М.: ЮНИТИ, 2004. – 573 с.

7. *Жданов*, *О.Н.* Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. – М.: ИНФРА-М, 2013. – 90 с.

8. *Мазурков*, *М.И.* Нелинейные S-блоки подстановки на основе композиционных кодов степенных вычетов / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2013. – Т. 56, № 9. – С. 34–43.

Поступила в редакцию 24.03.15.