5. Вычислительная сложность атак на ACBF

В таблице приведён порядок $h(n)$ вычислительной сложности $\mathrm{O}(h(n))$ атаки, построенной по общей схеме на шифр и схему подписи в ACBF $\mathcal{C}(J)$ для каждого непустого подмножества ключевых параметров $J \subseteq I$. Здесь $p(n)$ — некоторый полином от n.

J	$\{\sigma_1\}$	$\{\pi_1\}$	$\{\pi_1,\sigma_1\}$	$\{\sigma_2\}$	$\{\sigma_1,\sigma_2\}$	$\{\pi_1,\sigma_2\}$	$\{\pi_1,\sigma_1,\sigma_2\}$	$\{\pi_2\}$
$h(n)$	$p(n)$	$p(n)$	$\mathrm{C}_n^{n/2}$	$p(n)$	2^n	$\mathrm{C}_n^{n/2}$	$2^n\mathrm{C}_n^{n/2}$	$p(n)$

J	$\{\pi_2,\sigma_1\}$	$\{\pi_1,\pi_2\}$	$\{\pi_1,\pi_2,\sigma_1\}$	$\{\pi_2,\sigma_2\}$	$\{\pi_2,\sigma_1,\sigma_2\}$	$\{\pi_1,\pi_2,\sigma_2\}$	$\{\pi_1,\pi_2,\sigma_1,\sigma_2\}$
$h(n)$	$\mathrm{C}_n^{n/2}$	$n!$	$n!$	$p(n)$	2^n	$n!$	$n!2^n$

ЛИТЕРАТУРА

1. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 40. С. 23–33.
2. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
3. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 4–9.
4. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского государственного университета. Приложение. 2003. № 6. С. 31–41.

УДК 519.1 DOI 10.17223/2226308X/11/18

О СВОЙСТВАХ ДВУХ КЛАССОВ S-БОКСОВ РАЗМЕРА 16×16

В. М. Бобров, С. М. Комиссаров

Нелинейные отображения векторного пространства V_n (s-боксы размера $n \times n$) в симметричных алгоритмах блочного шифрования обычно реализуются в виде таблиц, содержащих множество всех образов. Для хранения одного такого массива требуется $n2^n$ бит памяти. Это вынуждает в алгоритмах блочного шифрования использовать s-боксы малых размеров (8×8 бит в алгоритме «Кузнечик», 4×4 в алгоритме «Магма», 6×4 в DES, 8×8 в AES). Предложена алгоритмическая реализация s-боксов 16×16 бит на основе функции модифицированного аддитивного генератора, а также на основе легковесного алгоритма блочного шифрования NASH. Лучшая максимальная разностная характеристика построенных s-боксов равна $18/2^{16}$. Минимальная степень нелинейности среди координатных функций равна 15. Минимальная степень нелинейности среди всех нетривиальных линейных комбинаций координатных функций равна 14–15. Лучшая линейная характеристика равна $764/2^{15}$.

Ключевые слова: *модифицированный аддитивный генератор, алгоритм NASH, s-бокс, максимальная разностная характеристика, максимальная линейная характеристика, степень нелинейности.*

Обозначим V_n — n-мерное векторное пространство над полем GF(2). Пусть $V_n^\times = V_n \backslash \{0\}$. Для некоторого вектора $a \in V_n$ определим линейную булеву функцию $l_a : V_n \to \mathrm{GF}(2)$:

$$l_a(x) = \bigoplus_{i=0}^{n-1} a_i \cdot x_i.$$

Корреляцию двух булевых функций f_1 и f_2 обозначим как

$$c(f_1, f_2) = 2^{1-n}|\{x : f_1(x) = f_2(x)\}| - 1.$$

Исследованы следующие характеристики подстановок $s : V_{16} \to V_{16}$:

1) совершенность, или существенная зависимость каждой координатной функции от всех переменных;
2) минимальная степень нелинейности среди всех координатных функций;
3) максимальная разностная характеристика, вычисляемая по формуле

$$p_s = 2^{-n} \cdot \max_{\alpha,\beta \in V_n^\times} |\{x \in V_n : s(x \oplus \alpha) \oplus s(x) = \beta\}|;$$

4) линейная характеристика, вычисляемая по формуле

$$\delta_s = \max_{\alpha,\beta \in V_n^\times} |c(l_\alpha, l_\beta(s(x))|;$$

5) минимальная степень нелинейности среди всех нетривиальных линейных комбинаций координатных функций, вычисляемая по формуле

$$\lambda_s = \min_{\alpha \in V_n^\times} \{\deg(l_\alpha(s(x)))\}.$$

1. Построение s-бокса 16×16 на основе модифицированного аддитивного генератора

Используем подход, аналогичный описанному в [1].

Обозначим: $m = 2^{16}$; $X_0, \ldots, X_{r-1}$ — знаки начального состояния модифицированного аддитивного генератора (МАГ) длины r (числа кольца вычетов Z_m); b — биекция, определяющая двоичное 16-разрядное представление числа X по правилу: если $X = 2^{15}x_0 + \ldots + 2x_{14} + x_{15}$, то $b(X) = \bar{X} = (x_0, \ldots, x_{15}) \in V_{16}$; g — преобразование множества V_{16} (модификация аддитивного генератора); φ^g — преобразование регистра сдвига длины r над V^{16}, реализуемое МАГ:

$$\varphi^g(\bar{X}_0, \ldots, \bar{X}_{r-1}) = (\bar{X}_1, \ldots, \bar{X}_{r-1}, bg((\bar{X}_0 + \bar{X}_{r-1}) \bmod m)).$$

Знаки гаммы X_i, генерируемые МАГ, образуются по закону рекурсии:

$$X_i = bgb^{-1}((X_{i-1} + X_{i-r}) \bmod m),\ i \geqslant r. \tag{1}$$

При фиксации переменных $\bar{X}_0 = z_0, \ldots, \bar{X}_{r-2} = z_{r-2}$ реализуемая в соответствии с (1) функция $\bar{X}_{r-1} \to \bar{X}_{r-1+l}$ при $r - 1 \geqslant l \geqslant 1$ есть подстановка множества V_{16} [1, теорема 1]. Для краткости обозначим эту подстановку $s^{(l)}(z, x)$, где $z = (z_0, \ldots, z_{r-2}) \in V_{16(r-1)}$, $x = (x_0, \ldots, x_{15}) = \bar{X}_{r-1}$.

Экспериментально исследованы разные функции модификации, построенные с использованием конкатенации узлов замены ГОСТ 28147-89 [2]. В качестве s-бокса 16×16 исследовалась подстановка $s^{(l)}(z, x)$. Экспериментальные расчёты показали, что наилучшее соотношение скорости реализации и криптографических характеристик достигается при следующей функции модификации:

$$g(x_0, \ldots, x_{15}) =$$
$$= (S(x_1 \oplus x_6 \oplus x_{11} \oplus x_{12}, x_2 \oplus x_7 \oplus x_8 \oplus x_{13}, x_3 \oplus x_4 \oplus x_9 \oplus x_{14}, x_0 \oplus x_5 \oplus x_{10} \oplus x_{15}),$$
$$S(x_1 \oplus x_{11} \oplus x_{12}, x_2 \oplus x_8 \oplus x_{13}, x_3 \oplus x_9 \oplus x_{14}, x_0 \oplus x_{10} \oplus x_{15}),$$
$$S(x_1 \oplus x_6 \oplus x_{12}, x_2 \oplus x_7 \oplus x_{13}, x_3 \oplus x_4 \oplus x_{14}, x_0 \oplus x_5 \oplus x_{15}),$$
$$S(x_1 \oplus x_6 \oplus x_{11}, x_2 \oplus x_7 \oplus x_8, x_3 \oplus x_4 \oplus x_9, x_0 \oplus x_5 \oplus x_{10})),$$

где S — узел замен ГОСТ 28147-89, и значениях $r = 4$ и $l = 3$. При данной модификации перемешивающая матрица МАГ является J^2-положительной, где $J = \{16(r-1), \ldots, 16r-1\}$ [3].

Рассчитаны некоторые криптографические характеристики исследуемых подстановок. Для нескольких узлов замены посчитаны разностные характеристики при 1000 фиксаций z. Подстановки брались с одинаковыми фиксациями z для всех узлов замены. В табл. 1 и 2 приведены распределения разностных характеристик для первого и второго узла.

Таблица 1

Разностные характеристики, узел замен 1

Значение $p_s \cdot 2^{16}$	18	20	22	24	26	28	30	32	34	36	38	40	42
Число подстановок	22	146	249	234	157	102	45	22	12	4	3	2	2
Среднее значение $p_s \cdot 2^{16}$	24,232												

Таблица 2

Разностные характеристики, узел замен 2

Значение $p_s \cdot 2^{16}$	18	20	22	24	26	28	30	32	34	38
Число подстановок	97	393	260	144	60	28	10	6	1	1
Среднее значение $p_s \cdot 2^{16}$	21,690									

При всех исследованных функциях модификации и параметрах МАГ наименьшая полученная разностная характеристика равна $18/2^{16}$. Среднее значение разностной характеристики ниже при использовании узлов замены с большей степенью нелинейности.

Для всех подстановок, использующих второй узел замен и имеющих разностную характеристику $18/2^{16}$, рассчитана степень нелинейности λ_s. Для всех исследованных подстановок $\lambda_s = 14$ или 15.

Проверено 20 подстановок для узла замен 2 . Наименьшая полученная линейная характеристика $\delta_s = 764/2^{15}$, наибольшая — $950/2^{15}$.

2. Построение s-бокса 16×16 на основе алгоритма NASH

Итеративный алгоритм блочного шифрования NASH [4] основан на принципах современной «легковесной криптографии». Его отличительной особенностью является использование в раундовой функции циклического сдвига на переменное число бит в зависимости от текущего блока и подключа, что позволяет, по словам авторов алгоритма, при сохранении уровня стойкости уменьшить количество раундов.

s-Бокс на основе алгоритма NASH представляет собой сеть Фейстеля, функция усложнения которой состоит из сложения по модулю 2^n, где n — размер полублока (в данном случае 8), с некоторой константой и циклического сдвига на переменное число бит. Преобразование блока на i-м раунде можно представить следующими формулами:

$$R_{i+1} = L_i, \quad L_{i+1} = ((L_i \boxplus C) \ggg F(L_i, L_i \boxplus C)) \oplus R_i,$$

где L_i и R_i — левый и правый полублоки шифруемого блока на i-м цикле преобразования соответственно; C — константа; F — функция управления сдвигами, которая выбирает одно из четырёх значений величины циклического сдвига полублока; $\boxplus$ —

сложение по модулю 2^n. Для получения первого бита функция F выбирает из полублока $L_i \boxplus C$ биты с номерами $2^k - 1$, $k = 1, \ldots, n$. Затем, интерпретируя полублок L_i размера 2^n бит как вектор значений булевой функции от n переменных, получает значение первого бита как значение этой функции на векторе бит из $L_i \boxplus C$ с номерами $2^1 - 1, 2^2 - 1, \ldots, 2^n - 1$, где порядок следования бит — от старшего к младшему. Затем полублоки L_i и $L_i \boxplus C$ меняются местами и второй бит выбирается аналогично. По значениям полученных битов выбирается одно из четырёх значений, на которое производится циклический сдвиг.

С помощью матрично-графового подхода [5, гл. 10] оценено, а затем экспериментально подтверждено, что для достижения совершенности произведения раундовых подстановок требуется четыре итерации.

При различном количестве итераций s-бокса, разных значениях циклического сдвига и переборе константы C от 0 до 255 проверены первые три характеристики для более чем 16000 подстановок. Минимальная степень нелинейности среди всех координатных функций для большинства подстановок, в том числе для всех подстановок с лучшими разностными характеристиками, равна 15. При фиксации сдвигов значениями $1, 2, 3, 4$ и переборе константы от 0 до 255 для всех подстановок, за исключением двух, параметр λ_s равен 14 или 15. Лучшие разностные характеристики для разного количества итераций приведены в табл. 3.

Таблица 3

Количество итераций s-бокса	4	5	6	7	8
Лучшее значение p_s	$200/2^{16}$	$40/2^{16}$	$20/2^{16}$	$20/2^{16}$	$18/2^{16}$

При дальнейшем увеличении количества итераций не найдено разностной характеристики меньше $18/2^{16}$. Кроме того, в каждой исследованной подстановке это значение характеристики встречается либо один раз, либо ни разу.

Для некоторых подстановок с лучшими разностными характеристиками исследована линейная характеристика. Для шести раундов для сдвигов $1, 2, 3, 4$ при фиксации константы $C = 105$ ($p_s = 20$) линейная характеристика равна $\delta_s = 946/2^{15}$. Для сдвигов $1, 4, 2, 3$ при восьми итерациях при фиксации константы $C = 215$ ($p_s = 18$) линейная характеристика равна $\delta_s = 860/2^{15}$.

В табл. 4–6 приведено сравнение полученных характеристик с характеристиками известных s-боксов. Производительность оценивалась как скорость обработки большого объема данных одним s-боксом 16×16 и двумя s-боксами 8×8 алгоритма «Кузнечик».

Таблица 4

Сравнение максимальных разностных характеристик построенных s-боксов с известными s-боксами

s-бокс	AES, 8×8	Skipjack, 8×8	«Кузнечик», 8×8	[6], 8×8	Данная работа, 16×16	Табличная реализация из [7], 16×16
p_s	$1{,}6 \cdot 10^{-2}$	$4{,}7 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-2}$	$2{,}3 \cdot 10^{-2}$	$2{,}7 \cdot 10^{-4}$	$6{,}1 \cdot 10^{-5}$

Таблица 5

Сравнение линейных характеристик s-боксов из данной работы с известными s-боксами

s-бокс	AES, 8×8	Skipjack, «Кузнечик», 8×8	[6], 8×8	s-бокс 16×16 на основе NASH	s-бокс 16×16 на основе МАГ	Табличная реализация из [7], 16×16
δ_s	$12{,}5 \cdot 10^{-2}$	$21{,}9 \cdot 10^{-2}$	$18{,}8 \cdot 10^{-2}$	$2{,}6 \cdot 10^{-2}$	$2{,}3 \cdot 10^{-2}$	$0{,}8 \cdot 10^{-2}$

Таблица 6

Сравнение производительности построенных s-боксов (Intel Core i7-7700K, 4,2 ГГц)

s-бокс	16×16 на основе МАГ	16×16 на основе NASH				8×8 алгоритма «Кузнечик»
		4 раунда	5 раундов	6 раундов	8 раундов	
Мбайт/с	136,239	146,719	127,156	105,963	76,293	476,837

Выводы

Предложенные s-боксы 16×16 обладают рядом положительных криптографических свойств: высокой степенью нелинейности, низкими максимальной разностной и линейной характеристиками. Они также отличаются простотой программной реализации. Их использование в итеративных алгоритмах блочного шифрования позволит снизить затраты памяти при программной реализации (на хранение прямого и обратного s-боксов 16×16, как, например, в [7], требуется 256 кбайт памяти), а также улучшить перемешивающие свойства раундового преобразования и его стойкость к различным видам криптоанализа. Вместе с тем полученные на данный момент способы алгоритмической реализации s-боксов 16×16 в 3,5–5 раз уступают в производительности табличным реализациям.

ЛИТЕРАТУРА

1. *Фомичев В. М., Лолич Д. М., Юзбашев А. В.* Алгоритмическая реализация s-боксов на основе модифицированных аддитивных генераторов // Прикладная дискретная математика. Приложение. 2017. № 10. С. 102–104.
2. Методические рекомендации ТК26. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89. М., 2013. `https://tc26.ru/standarts/metodicheskie-rekomendatsii/zadanie-uzlov-zameny-bloka-podstanovki-algoritma-shifrovaniya-gost-28147-89.html`
3. *Фомичев В. М., Кяжин С. Н,* Локальная примитивность матриц и графов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1. С. 97–119.
4. *Lebedev A., Karondeev A., and Kozlov A.* New Block Cipher [Электронный ресурс]. `https://ist.ac.at/eurocrypt2016/slides/121.pdf`
5. *Фомичев В. М.* Методы дискретной математики в криптологии: учеб. пособие. М.: Диалог-МИФИ, 2010.
6. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-boxes // CTCrypt Preproc. Yaroslavl, 2016. P. 232–252. `https://mjos.fi/doc/rus/CTCrypt2016Preproceedings.pdf`
7. *Wood C. A.* Large Substitution Boxes with Efficient Combinational Implementations. Thesis. Rochester Institute of Technology, 2013.