УДК 519.1 DOI 10.17223/2226308X/10/41

АЛГОРИТМИЧЕСКАЯ РЕАЛИЗАЦИЯ s-БОКСОВ НА ОСНОВЕ МОДИФИЦИРОВАННЫХ АДДИТИВНЫХ ГЕНЕРАТОРОВ[1]

В. М. Фомичев, Д. М. Лолич, А. В. Юзбашев

Предложен алгоритмический способ реализации s-боксов (в том числе большого размера) на основе модифицированных аддитивных генераторов (МАГ). Свойства полученных подстановок обоснованы как с помощью алгебраических и перемешивающих свойств МАГ, так и с помощью эксперимента на ЭВМ. Проверены следующие свойства сгенерированных подстановок: 1) совершенность (существенная зависимость координатных функций от всех переменных; 2) нелинейность всех нетривиальных линейных комбинаций координатных функций; 3) близость максимальной разностной характеристики к максимальной разностной характеристике случайной подстановки. С использованием МАГ и нескольких отобранных s-боксов 4×4 сгенерированы и исследованы около 2^{19} s-боксов 8×8. Почти все они имеют свойства 1 и 2. Для большого количества (несколько тысяч) построенных s-боксов 8×8 максимальная разностная характеристика равна $10/256$ и для четырёх s-боксов — $8/256$. Данный подход позволяет строить s-боксы большего размера.

Ключевые слова: *модифицированный аддитивный генератор, МАГ, s-бокс, регистр сдвига.*

1. Построение подстановок с помощью МАГ

Критически важные узлы замены симметричных итеративных блочных шифров (s-боксы), обеспечивающие нелинейность и полное перемешивание входных данных, задаются, как правило, таблично и реализуют отображения двоичных векторных пространств малой размерности (6×4 битов в алгоритме DES, 4×4 битов в ГОСТ 28147-89, 8×8 битов в алгоритме «Кузнечик»). Размер s-боксов ограничен в силу ресурсоёмкости их табличной реализации по размеру памяти и времени.

Для построения s-боксов использованы МАГ длины 3 с точками съёма 0 и 2 и МАГ длины 4 с точками съёма 0 и 3 [1].

Обозначим: $X_0, \ldots, X_{n-1}$ — знаки начального состояния МАГ длины n (числа кольца вычетов $\mathbb{Z}_{256}$; b — биекция, определяющая двоичное 8-разрядное представление числа $X \in \mathbb{Z}_{256}$ по правилу: если $X = 2^7x_0 + \ldots + 2x_6 + x_7$, то $b(X) = \overline{X} = (x_0, \ldots, x_7) \in V_8$; g — преобразование множества V_8 (модификация аддитивного генератора); ϕ^g — преобразование регистра сдвига длины n над V_8, реализуемое МАГ:

$$\phi^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, \overline{X}_{n-1}, bg((X_0 + X_{n-1}) \bmod 256)).$$

Перемешивающий орграф $\Gamma(\phi^g)$ преобразования ϕ^g имеет $8n$ вершин, где разрядам числа X_i соответствует множество вершин $\{8i, 8i+1, \ldots, 8i+7\}$, $i = 0, \ldots, n-1$.

Преобразование ϕ^g — подстановка, если и только если g — подстановка [1]. Знаки гаммы X_i, генерируемые МАГ, образуются по закону рекурсии

$$X_i = bgb^{-1}((X_{i-1} + X_{i-n}) \bmod 256), \quad i \geqslant n. \tag{1}$$

При фиксации переменных $\overline{X}_0 = z_0, \ldots, \overline{X}_{n-2} = z_{n-2}$ реализуемая в соответствии с (1) функция $\overline{X}_{n-1} \to \overline{X}_{n-1+l}$ при любом $l \geqslant 1$ есть преобразование множества V_8.

[1]Работа первого автора выполнена в соответствии с грантом РФФИ № 16-01-00226.

Для краткости обозначим это преобразование $s^{(l)}(z,x)$, где $z=(z_0,\dots,z_{n-2})\in V_{8(n-1)}$, $x=(x_0,\dots,x_7)=\overline{X}_{n-1}$.

Теорема 1. Пусть 0, $n-1$ — точки съёма МАГ, g — подстановка. Тогда при $l=1,\dots,n-1$ и при любой фиксации z преобразование $s^{(l)}(z,x)$ есть подстановка множества V_8.

2. Способ построения подстановок

Для построения s-боксов размера 8×8 использованы s-боксы 4×4 и модификации $g(x_0,\dots,x_7)=(K(x_0\oplus x_4,x_1\oplus x_5,x_2\oplus x_6,x_3\oplus x_7),K(x_0,x_1,x_2,x_3))$, где $K\in\{K_1,\dots,K_8,E_1,\dots,E_8,I_1,\dots,I_8\}$, K_i — узлы замены ГОСТ 28147-89 [2], E_i,I_i — узлы шифра Serpent [3], $i=1,\dots,8$. Каждому узлу замены соответствует $2^{8(n-1)}$ подстановок вида $s^{(l)}(z,x)$, $l=1,\dots,n-1$. Перемешивающие свойства подстановок оценены с помощью локального экспонента [4].

Теорема 2. Пусть $g(x_0,\dots,x_7)=(K(x_0\oplus x_4,x_1\oplus x_5,x_2\oplus x_6,x_3\oplus x_7),K(x_0,x_1,x_2,x_3))$, где K — совершенный s-бокс 4×4; 0 и $n-1$ — точки съёма МАГ. Тогда при $J=\{8n-8,8n-7,\dots,8n-1\}$ локальный экспонент J^2-$\exp\Gamma=2$.

3. Экспериментальное исследование свойств сгенерированных подстановок

С помощью теорем 1 и 2 сделан обоснованный выбор параметра $l=2$ при $n=3$ и $l=3$ при $n=4$. С помощью программной реализации МАГ на ЭВМ для каждого узла замены получены все 2^{16} подстановок при $n=3$ и 2^{19} подстановок (выборочно) при $n=4$. Для каждой подстановки s с координатными функциями $s_1,\dots,s_8$ проверены следующие свойства:

1) совершенность (существенная зависимость функции s_j от переменных x_i, $i,j=1,\dots,8$;
2) нелинейность всех нетривиальных линейных комбинаций функций $s_1,\dots,s_8$;
3) близость максимальной разностной характеристики p_s к максимальной разностной характеристике случайной подстановки, где $p_s=\max\limits_{\alpha,\beta\in V_8}|\{x\in V_8: s(x)\oplus s(x\oplus\alpha)=\beta\}|$.

Установлено, что свойства 1, 2 имеют большинство подстановок (при $n=3$ не имеют 1088 подстановок, соответствующих узлу I_1, и менее 400 — любому другому узлу).

Характеристика p_s подстановок при $n=3$ принимает значения $(10+2k)/256$, $k=0,1,\dots,15$. В табл. 1 приведено число полученных при $n=3$ подстановок s, для которых $p_s=10/256$.

Таблица 1

Число подстановок со свойствами 1, 2 и характеристикой $p_s=10/256$, $n=3$

Узлы замены	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8
Число подстановок	44	24	68	100	24	48	84	48	32	12	20	128	152	140	4	64	104	116	8	160	92	124	44	80

При $n=3$ посчитано, что обратные подстановки (к каждой подстановке табл. 1) обладают свойствами 1, 2 и их разностная характеристика p_s также равна $10/256$.

При $n=4$ характеристики p_s подстановок принимают значения $(8+2k)/256$, $k=0,1,\dots$; в табл. 2 приведены количества подстановок для $k=0$ и 1.

Сравним характеристики p_s у полученных и известных s-боксов размера 8×8 (табл. 3). Видим, что характеристики p_s полученных с помощью МАГ подстановок s

Таблица 2

Число подстановок со свойствами 1, 2 и характеристикой $p_s \in \{8/256, 10/256\}$, $n = 4$

p_s	Узлы замены, использованные в МАГ							
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8
8/256	0	2	0	0	0	0	0	2
10/256	18615	19968	20309	19921	20107	18898	18506	19807

близки по порядку к характеристике 6/256 наилучших на сегодняшний день s-боксов [5]. Заметим, что величина $p_s = 10/256$ соответствует большому количеству случайных подстановок степени 256 и не превышает их среднего значения [5, табл. 1].

Таблица 3

Сравнение характеристик p_s для s-боксов известных алгоритмов

Алгоритм	«Skipjack»	«Кузнечик»	s-боксы работы [5]	s-боксы табл. 1 и 2
p_s	12/256	8/256	6/256	8/256, 10/256

Выводы

Алгоритмический подход позволяет построить с использованием МАГ и s-боксов 4×4 большое количество s-боксов 8×8 с рядом позитивных криптографических свойств. Представляется перспективным совершенствование характеристик s-боксов 8×8 за счёт изменения параметров схемы построения и исследование вопросов синтеза s-боксов больших размеров (16×16, 32×32 и др.).

ЛИТЕРАТУРА

1. *Коренева А. М., Фомичев В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 2. С. 47–67.
2. Рекомендации по стандартизации. Задание узлов замены блока подстановки алгоритма шифрования ГОСТ 28147-89. М., 2013.
3. *Anderson R., Biham E., and Knudsen L. R.* Serpent: A Proposal for the Advanced Encryption Standard. NIST AES Proposal, 1998.
4. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и графов // Дискрет. анализ и исслед. операций. 2017. Т. 24. № 1. С. 97–119.
5. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-boxes // CTCrypt Preproceedings. Yaroslavl, 2016. P. 232–252.

УДК 519.1 DOI 10.17223/2226308X/10/42

О ПОСТРОЕНИИ S-БОКСОВ РАЗМЕРА 4×4[1]

В. М. Фомичев, П. В. Овчинников

Предложен и реализован метод построения всех s-боксов размера 4×4, для которых выполнены следующие криптографические свойства: 1) биективность; 2) отсутствие неподвижных точек; 3) нелинейность всех нетривиальных линейных комбинаций вида координатных функций; 4) значение разностной характеристики p_s

[1]Работа первого автора выполнена в соответствии с грантом РФФИ № 16-01-00226.