УДК 519.1 DOI 10.17223/2226308X/12/32

ОБ АЛГОРИТМИЧЕСКОЙ РЕАЛИЗАЦИИ S-БОКСОВ 16×16 СО СТРУКТУРАМИ ARX И «БАБОЧКА»

С. М. Комиссаров

Предложены способы алгоритмической реализации новых s-боксов размера 16×16 бит, вычислительная сложность и криптографические характеристики которых улучшены по сравнению со способами, исследованными ранее. Первый способ реализует s-боксы на основе ARX (Add-Rotate-Xor)-структуры; второй — на основе структуры «Бабочка» с использованием нелинейных подстановочных s-боксов размера 8×8 бит. Максимальная разностная характеристика (МРХ) предложенных s-боксов с ARX-структурой равна $18/2^{16}$, со структурой «Бабочка» — $10/2^{16}$. Максимальная линейная характеристика (МЛХ) s-боксов с ARX-структурой равна $764/2^{15}$, со структурой «Бабочка» — $512/2^{15}$. Минимальная степень нелинейности среди всех нетривиальных линейных комбинаций координатных функций предложенных s-боксов равна 15. Установлено, что использование предложенных s-боксов размера 16×16 бит в раундовых подстановках алгоритмов AES и «Кузнечик» позволяет улучшить их некоторые криптографические свойства. Для усечённых алгоритмов AES и «Кузнечик», реализующих несколько раундов шифрования, существенно снижены верхние оценки МРХ и МЛХ по сравнению с версиями алгоритмов, использующих штатные s-боксы.

Ключевые слова: *s-бокс* 16×16*, алгоритмическая реализация, ARX, «Бабочка», максимальная разностная характеристика, максимальная линейная характеристика, степень нелинейности.*

Цель работы — оценить важнейшие характеристики некоторых способов реализации s-боксов (узлов замены) размера 16×16 бит и перспективы их использования в итеративных алгоритмах блочного шифрования.

Нелинейные отображения векторного пространства V_n (s-боксы размера $n \times n$ бит) в симметричных алгоритмах блочного шифрования обычно реализуются в виде таблиц, содержащих множество всех образов. Для хранения одного такого массива требуется n^2 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). В данной работе предложены способы алгоритмической реализации новых s-боксов большого размера (16×16 бит). При алгоритмическом вычислении значений s-боксов больших затрат памяти не требуется.

Обозначим $b : \mathbb{Z}_{2^n} \to V_n$ — биективное отображение числа $X \in \mathbb{Z}_{2^n}$ в его двоичное представление, $b(X) = \bar{X} = (x_0, \ldots, x_{n-1})$; $(\bar{X}_1, \bar{X}_2)$ — конкатенация двух векторов; $X_1, X_2 \in \mathbb{Z}_{2^n}$ — полублоки входного блока X s-бокса, $X = (X_1, X_2) \in \mathbb{Z}_{2^{16}}$; $b(X_1) = \bar{X}_1 = (x_0, \ldots, x_7)$, $b(X_2) = \bar{X}_2 = (x_8, \ldots, x_{15})$, $b(X) = (x_0, \ldots, x_{15})$; $Y \ggg t$ ($Y \lll t$) — циклический сдвиг координат вектора Y на t бит вправо (влево); $\otimes$ — умножение в поле $\mathbb{F}(2^8) = \mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$; $a^{254} = a^{-1}$ — обратный к ненулевому элементу a поля $\mathbb{F}(2^8)$; $S : V_m \to V_m$ — функция s-бокса размера $m \times m$ бит.

Для $x \in V_m$ и $x' = x \oplus a \in V_m$ (пар текстов с фиксированной разностью $a \in V_m$) и s-бокса $S : V_m \to V_m$ определим разностную характеристику (РХ) $DP^S(a, b) = |\{x \in V_m : S(x) \oplus S(x') = b\}|/2^m$ — вероятность появления случайной величины — разности $b \in V_m$ выходных текстов $S(x)$ и $S(x')$. Максимальная разностная характеристика (МРХ) s-бокса определена как $p_s = \max\limits_{a,b \in V_m^{\times}} DP^S(a, b)$. Для векто-

ра $a = (a_0, \ldots, a_{m-1}) \in V_m$ определим линейную булеву функцию $l_a(x_0, \ldots, x_{m-1}) = \bigoplus_{i=0}^{m-1} a_i x_i$. Для некоторых $a, b \in V_m$ и s-бокса $S : V_m \to V_m$ с компонентными функциями $(S_0, \ldots, S_{m-1})$ определим линейную характеристику (ЛХ) $LP^S(a,b) = 2^{1-m}|\{x \in V_m : l_a(x) = l_b(S(x))\}| - 1$. Максимальную линейную характеристику (МЛХ) s-бокса S определим как $\delta_S = \max_{a,b \in V_m^\times} LP^S(a,b)$. Пусть $\deg f$ — степень нелинейности функции f. Минимальная степень нелинейности среди всевозможных линейных комбинаций координатных функций определена в [1] как $\lambda_S = \min_{a,b \in V_m^\times} \{\deg(l_a(S(x)))\}$. Производительность s-боксов измеряется в Мбайт/с, ёмкость памяти — в байтах.

Алгоритмы AES и «Кузнечик» при использовании в них s-боксов размера 16×16 бит вместо стандартных обозначим AES16 и K16.

1. Описание метода алгоритмической реализации s-бокса 16×16 с ARX-структурой

s-Боксы на основе ARX-структуры используют операции сложения, циклического сдвига и побитового XOR-сложения векторов. Эти операции не требуют существенных затрат памяти на хранение предварительно вычисленных таблиц [2, 3], характеризуются низкой ресурсоёмкостью в программных и аппаратных реализациях и выполняются менее чем за половину такта процессора.

Раундовые подстановки $g_i : V_{16} \to V_{16}$, $i = 1, 2$, s-боксов 16×16 с ARX-структурой, предлагаемые в данной работе, в общем виде представимы в виде композиции двух преобразований $f_{i1}, f_{i2} : V_{16} \to V_{16}$:

$$g_i(X) = f_{i2} \circ f_{i1}(X). \tag{1}$$

Построены перспективные схемы с ARX-структурой с точки зрения сочетания положительных криптографических характеристик с высокой производительностью программной реализации.

Первый вариант раундового преобразования (1) s-бокса обозначим g_1, для него

$$f_{11}(X) = (b(((X_1 \ggg 2) + X_2) \bmod 2^8), \bar{X}_2),\ f_{12}(X) = (\bar{X}_1, b(((X_2 \lll 1) + C) \bmod 2^8) \oplus \bar{X}_1).$$

Второй вариант раундового преобразования (1) s-бокса обозначим g_2, для него

$$f_{21}(X) = (b(((X_1 \lll 1) + X_2) \bmod 2^8), \bar{X}_2),\ f_{22}(X) = (\bar{X}_1, b(((X_2 \ggg 2) + C) \bmod 2^8) \oplus \bar{X}_1).$$

Здесь $C \in \mathbb{Z}_{2^8}$ — константа, $C = 185$ для g_1 и $C = 100$ для g_2. Обозначим $\varphi_1 = g_1^6$, $\varphi_2 = g_2^6$ — предложенные s-боксы с ARX-структурой.

Экспериментально установлено, что для предложенных s-боксов $p_{\varphi_1} = p_{\varphi_2} = 18/2^{16}$, $\delta_{\varphi_1} = 762/2^{15}$, $\delta_{\varphi_2} = 764/2^{15}$, $\lambda_{\varphi_1} = \lambda_{\varphi_2} = 15$.

В табл. 1 приведены частоты значений DP в таблицах разностей φ_1 и φ_2. Видно, что частота встречаемости MPX невелика, поэтому при реализации разностной атаки сложно подобрать несколько s-боксов с MPX более чем в одном рауде шифрования.

Таблица 1

Частота встречаемости значений DP в таблицах разностей φ_1 и φ_2

$2^{16} \cdot DP$	0	2	4	6	8	10	12	14	16	18
φ_1	$2{,}6 \cdot 10^9$	$1{,}3 \cdot 10^9$	$3{,}3 \cdot 10^8$	$5{,}4 \cdot 10^7$	$6{,}8 \cdot 10^6$	678529	56603	4062	280	14
φ_2	$2{,}6 \cdot 10^9$	$1{,}3 \cdot 10^9$	$3{,}3 \cdot 10^8$	$5{,}4 \cdot 10^7$	$6{,}8 \cdot 10^6$	677386	56885	4058	256	7

2. Об алгоритмической реализации s-бокса 16×16 со структурой «Бабочка»

В [4, 5] предложены способы построения s-боксов 8×8 со структурой «Бабочка» с использованием умножения в $\mathrm{GF}(2^4)$ и подстановок меньших размеров (4×4 бит), реализующих мономы в $\mathrm{GF}(2^4)$. В данной работе предложены два типа s-боксов 16×16 со структурой «Бабочка» с использованием умножения в $\mathrm{GF}(2^8)$ и подстановок меньших размеров (8×8 бит), реализующих мономы в $\mathrm{GF}(2^8)$. Обозначим $\psi_i : V_{16} \to V_{16}$, $i = 1, 2$:

$$\psi_i(X) = \psi_i(\bar{X}_1, \bar{X}_2) = (b(F_{i1}(X_1, X_2)), b(F_{i2}(X_2, F_{i1}(X_1, X_2)))) = (\bar{X}'_1, \bar{X}'_2).$$

За основу первого типа s-боксов 16×16 взята структура из [4]. Обозначим его ψ_1, для него

$$F_{11}(X_1, X_2) = X'_1 = \begin{cases} h_1(X_1), & X_2 = 0, \\ (X_1 \otimes X_2)^{254}, & X_2 \neq 0, \end{cases}$$

$$F_{12}(X_2, X'_1) = X'_2 = \begin{cases} h_2(X_2), & X'_1 = 0, \\ X'_1 \otimes (X_2)^{254}, & X'_1 \neq 0, \end{cases}$$

где $F_{11}(X_1, X_2), F_{12}(X_2, X_1) : \mathbb{F}(2^{16}) \to \mathbb{F}(2^8)$ — биективные функции по X_1 и X_2 соответственно; $h_1, h_2 : \mathbb{F}(2^8) \to \mathbb{F}(2^8)$ — нелинейные подстановки, реализующие мономы в $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$. При $h_2(x) \in \{x^{254}, x^{253}\}$ и $h_1(x) = x^k$, где $k \in \{28, 37, 56, 73, 74, 131, 146, 148, 164, 191, 193, 239, 247, 251, 253, 254\}$, отображение ψ_1 биективно, $p_{\psi_1} = 10/2^{16}$, $\lambda_{\psi_1} = 15$ и $\delta_{\psi_1} = 512/2^{15}$.

За основу второго типа s-боксов 16×16 взята структура из [5]. Обозначим его ψ_2, для него

$$F_{21}(X_1, X_2) = X'_1 = \begin{cases} (X_1)^{254}, & X_2 = 0, \\ X_1 \otimes h_1(X_2), & X_2 \neq 0, \end{cases}$$

$$F_{22}(X_2, X'_1) = X'_2 = \begin{cases} (X_2)^{254}, & X'_1 = 0, \\ X_2 \otimes h_2(X'_1), & X'_1 \neq 0, \end{cases}$$

где $F_{21}(X_1, X_2), F_{22}(X_2, X_1) : \mathbb{F}(2^{16}) \to \mathbb{F}(2^8)$ — биективные функции по X_1 и X_2 соответственно. При $h_2(x) = x^{254}$ и $h_1(x) = x^2$ отображение ψ_2 биективно, $p_{\psi_2} = 10/2^{16}$, $\lambda_{\psi_2} = 15$ и $\delta_{\psi_2} = 512/2^{15}$. При $h_2(x) \in \{x^{254}, x^{253}\}$ и $h_1(x) \in \{x^{32}, x^{16}\}$ отображение ψ_2 биективно, $p_{\psi_2} = 10/2^{16}$, $\lambda_{\psi_2} = 15$ и $\delta_{\psi_2} = 544/2^{15}$.

При алгоритмической реализации ψ_1 и ψ_2 мономы h_1, h_2 и x^{-1} реализуются в виде таблиц, каждая из которых занимает $8 \cdot 2^8$ бит памяти. Требуются также две предварительно рассчитанные таблицы подстановок 8×8 бит для быстрой реализации произведения в $\mathbb{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$. Обозначим ψ — s-бокс 16×16 со структурой «Бабочка», реализующий ψ_1 при $h_1 = h_2 = x^{254} = x^{-1}$. При алгоритмической реализации он требует одну предварительно рассчитанную таблицу, задающую моном x^{254}, и имеет следующие характеристики: $p_\psi = 10/2^{16}$, $\lambda_\psi = 15$ и $\delta_\psi = 512/2^{15}$. В табл. 2 приведено распределение разностных характеристик в его таблице разностей.

В табл. 3 приведено сравнение МРХ, МЛХ и минимальной степени нелинейности среди всевозможных линейных комбинаций компонентных функций известных и предложенных s-боксов.

Таблица 2

Частота встречаемости значений DP в таблице разностей ψ

$2^{16} \cdot DP$	0	2	4	6	8	10
ψ	2507045091	1602586456	12279975	171659076	1328564	2598

Таблица 3

Сравнение p_s, δ_s и λ_s для s-боксов

s-Бокс	AES	Skipjack	«Кузнечик»	φ_1	φ_2	ψ	x^{-1}, таблица [6]
Размер	8×8	8×8	8×8	16×16	16×16	16×16	16×16
p_s	$4/2^8$	$12/2^8$	$8/2^8$	$18/2^{16}$	$18/2^{16}$	$10/2^{16}$	$4/2^{16}$
δ_s	$12/2^7$	$28/2^7$	$28/2^7$	$762/2^{15}$	$764/2^{15}$	$512/2^{15}$	$256/2^{15}$
λ_s	7	6	7	15	15	15	15

3. Верхние оценки разностной и линейной характеристик для алгоритмов AES16 и K16

При реализации разностной атаки s-бокс называется активным для раунда итеративного алгоритма блочного шифрования, если разность поступающих на этом раунде ему на вход текстов не равна нулю.

Пусть $L : V_m^n \to V_m^n$ — линейное преобразование алгоритма блочного шифрования на основе SP-сети с размером блока $m{\cdot}n$ бит. Обозначим β_i, $i = 1, \ldots, 4$, число активных s-боксов на i-м раунде.

Степень ветвления (branch number) линейного преобразования L (обозначим β_2^L или β_2 в случае, когда L является композицией всех используемых в алгоритме линейных преобразований) есть

$$\beta_2^L = \min_{x \in V_n^*} \{w(x) + w(L(x))\},$$

где $w(x) = w(x_1, x_2, \ldots, x_n) = |\{x_i \neq 0 : x_i \in V_m, i = 1, \ldots, n\}|$.

Степень ветвления алгоритма блочного шифрования на основе SP-сети можно определить как минимальное возможное число активных s-боксов, участвующих в первых двух раундах шифрования. Известно [7], что для AES $\beta_2 = 5$, $\beta_4 = (\beta_2)^2 = 25$, для алгоритма «Кузнечик» $\beta_2 = 17$ [8]. Для AES16 $\beta_2 = 5$, $\beta_4 = 15$; для K16 $\beta_2 = 9$.

Обозначим $a^k, b^k \in V_m^n$ разности пар входных и выходных текстов размера mn бит k-го раунда алгоритма блочного шифрования на основе SP-сети с s-боксами $S_i : V_m \to V_m$, $i = 1, \ldots, n$; $DP_2(a^1, b^2)$ $(DP_4(a^1, b^4))$ — РХ двух (четырёх) раундов алгоритма шифрования на основе SP-сети; $LP_2(a^1, b^2)$ $(LP_4(a^1, b^4))$ — ЛХ двух (четырёх) раундов алгоритма шифрования на основе SP-сети.

Теорема 1 [9]. Для любой ненулевой разности $a^1 \in V_{m \cdot n}^{\times}$ пары входных текстов РХ двух раундов алгоритма шифрования на основе SP-сети верно неравенство

$$DP_2(a^1, b^2) \leqslant \max \left\{ \max_{1 \leqslant i \leqslant n} \max_{1 \leqslant u \leqslant 2^m - 1} \sum_{j=1}^{2^m - 1} \{DP^{S_i}(u, j)\}^{\beta_2}, \max_{1 \leqslant i \leqslant n} \max_{1 \leqslant u \leqslant 2^m - 1} \sum_{j=1}^{2^m - 1} \{DP^{S_i}(j, u)\}^{\beta_2} \right\}.$$

В табл. 4 и 5 приведено сравнение посчитанных по лемме 1 [9] и теореме 1 верхних оценок РХ двух и четырёх раундов AES16 и K16 с оценками версий алгоритмов, использующих штатные s-боксы.

Приведём другие оценки РХ/ЛХ двух и четырёх раундов AES16 и K16, основанные на МРХ/МЛХ используемого s-бокса, аналогичные оценкам AES в [7]. Обозна-

Таблица 4

Верхние оценки PX для AES и AES16 по теоремам [9]

Алгоритм	AES [9]	AES16 с φ_1	AES16 с φ_2	AES16 с ψ
$DP_2(a,b) \leqslant$	$1{,}234 \cdot 2^{-28}$	$1{,}177 \cdot 2^{-56}$	$1{,}217 \cdot 2^{-56}$	$1{,}362 \cdot 2^{-56}$
$DP_4(a,b) \leqslant$	$1{,}144 \cdot 2^{-111}$	$1{,}240 \cdot 2^{-209}$	$0{,}950 \cdot 2^{-208}$	$0{,}956 \cdot 2^{-208}$

Таблица 5

Оценки PX для алгоритмов «Кузнечик» и K16 по теоремам [9]

Алгоритм	«Кузнечик» [9]	K16 с φ_1	K16 с φ_2	K16 с ψ
$DP_2(a,b) \leqslant$	$0{,}909 \cdot 2^{-106}$	$0{,}932 \cdot 2^{-112}$	$1{,}395 \cdot 2^{-113}$	$1{,}015 \cdot 2^{-120}$

чим $DP_2^S(a,b), DP_4^S(a,b)$ ($LP_2^S(a,b), LP_4^S(a,b)$) PX (ЛХ) двух и четырёх раундов алгоритма шифрования на основе SP-сети, использующего единственный s-бокс S; φ — любой из предложенных s-боксов с ARX-структурой (φ_1 или φ_2). Для любой ненулевой разности $a \in V_{m \cdot n}^{\times}$ имеет место $DP_2^S(a,b) \leqslant p_S^{\beta_2}$, $LP_2^S(a,b) \leqslant \delta_S^{\beta_2}, DP_4^S(a,b) \leqslant p_S^{\beta_4}$, $LP_4^S(a,b) \leqslant \delta_S^{\beta_4}$ [7]. Для AES16:

$$DP_2^{\varphi}(a,b) \leqslant p_{\varphi}^{\beta_2} = (18 \cdot 2^{-16})^5 \approx 0{,}9 \cdot 2^{-59};\ DP_4^{\varphi}(a,b) \leqslant p_{\varphi}^{\beta_4} = (18 \cdot 2^{-16})^{15} \approx 1{,}46 \cdot 2^{-178};$$

$$DP_2^{\psi}(a,b) \lesssim 1{,}52 \cdot 2^{-64};\ DP_4^{\psi}(a,b) \lesssim 1{,}78 \cdot 2^{-191};$$

$$LP_2^{\varphi_1}(a,b) \leqslant \delta_{\varphi_1}^{\beta_2} = (762 \cdot 2^{-15})^5 \approx 0{,}913 \cdot 2^{-27};$$

$$LP_4^{\varphi_1}(a,b) \leqslant \delta_{\varphi_1}^{\beta_4} = (762 \cdot 2^{-15})^{15} \approx 1{,}521 \cdot 2^{-82};$$

$$LP_2^{\varphi_2}(a,b) \lesssim 0{,}924 \cdot 2^{-27};\ LP_4^{\varphi_2}(a,b) \lesssim 1{,}582 \cdot 2^{-82};\ LP_2^{\psi}(a,b) \leqslant 2^{-30};\ LP_4^{\psi}(a,b) \leqslant 2^{-90}.$$

Для K16:

$$DP_2^{\varphi}(a,b) \leqslant p_{\varphi}^{\beta_2} = (18 \cdot 2^{-16})^9 \approx 1{,}443 \cdot 2^{-107};\ LP_2^{\varphi_1}(a,b) \lesssim 1{,}119 \cdot 2^{-49};$$

$$LP_2^{\varphi_2}(a,b) \lesssim 1{,}146 \cdot 2^{-49};\ DP_2^{\psi}(a,b) \lesssim 0{,}931 \cdot 2^{-114};\ LP_2^{\psi}(a,b) \leqslant 2^{-54}.$$

В табл. 6 и 7 приведено сравнение полученных оценок с оценками версий алгоритмов, использующих штатные s-боксы, в табл. 8 и 9 — сравнение производительности и затрат памяти s-боксов.

Таблица 6

Оценки PX и ЛХ для AES и AES16 на основе MPX и MЛХ s-бокса

Алгоритм	AES [7]	AES16 с φ_1	AES16 с φ_2	AES16 с ψ
$DP_2(a,b) \leqslant$	2^{-30}	$0{,}9 \cdot 2^{-59}$	$0{,}9 \cdot 2^{-59}$	$1{,}52 \cdot 2^{-64}$
$DP_4(a,b) \leqslant$	2^{-150}	$1{,}46 \cdot 2^{-178}$	$1{,}46 \cdot 2^{-178}$	$1{,}78 \cdot 2^{-191}$
$LP_2(a,b) \leqslant$	2^{-15}	$0{,}913 \cdot 2^{-27}$	$0{,}924 \cdot 2^{-27}$	2^{-30}
$LP_4(a,b) \leqslant$	2^{-75}	$1{,}521 \cdot 2^{-82}$	$1{,}582 \cdot 2^{-82}$	2^{-90}

Таблица 7

Оценки PX и ЛХ для алгоритмов «Кузнечик» и K16 на основе MPX и MЛХ s-бокса

Алгоритм	«Кузнечик»	K16 с φ_1	K16 с φ_2	K16 с ψ
$DP_2(a,b) \leqslant$	2^{-85}	$1{,}443 \cdot 2^{-107}$	$1{,}443 \cdot 2^{-107}$	$0{,}931 \cdot 2^{-114}$
$LP_2(a,b) \leqslant$	$0{,}826 \cdot 2^{-27}$	$1{,}119 \cdot 2^{-49}$	$1{,}146 \cdot 2^{-49}$	2^{-54}

Таблица 8

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

s-Бокс	16×16 на основе МАГ [3]	16×16, φ_1	16×16, φ_2	16×16, ψ	8×8, «Кузнечик»
Мбайт/с	136,239	444,604	383,773	200,141	449,846

Таблица 9

Сравнение затрат памяти s-боксов

s-Бокс	16×16, φ_1, φ_2		16×16, ψ	16×16, табличный s-бокс [6]	8×8, «Кузнечик», AES
Память	код, x86	код, x64	768 байт	128 кбайт	256 байт
	74 байта	102 байта			

Выводы

Предложены новые конструкции s-боксов размера 16×16 бит: s-боксы на основе ARX-структуры, имеющие высокопроизводительную алгоритмическую реализацию, и s-боксы со структурой «Бабочка», использующие нелинейные подстановки меньшего размера — 8×8 бит. Предложенные s-боксы обладают рядом положительных криптографических свойств: высокой степенью нелинейности, низкой МРХ и МЛХ. МРХ предложенных s-боксов «Бабочка» равна $10/2^{16}$. Это наименьшее значение МРХ среди известных s-боксов 16×16, не реализующих поиск обратного элемента в конечном поле. В рамках вычислительного эксперимента производительность предложенных s-боксов с ARX-структурой не уступает производительности таблично реализуемого s-бокса 8×8. Предложенные s-боксы требуют небольшое количество памяти (75 байт на хранение машинных инструкций — ARX, 768 байт — «Бабочка»), в то время как табличная реализация s-бокса 16×16 требует 128 кбайт. Отмечено положительное влияние предложенных s-боксов на стойкость алгоритмов AES и «Кузнечик» к дифференциальному и линейному методам криптоанализа при их встраивании и существенное уменьшение верхних оценок максимальной разностной и линейной характеристик AES16 и K16. Данные результаты позволяют сделать предположение о возможности уменьшения количества раундов в рассмотренных стандартах блочного шифрования при встраивании в них s-боксов размера 16×16 бит с сохранением стойкости. Это позволит увеличить скорость шифрования с использованием рассмотренных алгоритмов.

Поиск новых конструкций нелинейных подстановок степени 2^{16} является перспективным направлением исследований.

ЛИТЕРАТУРА

1. *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
2. *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.
3. *Бобров В. М., Комиссаров С. М.* О свойствах двух классов s-боксов размера 16×16 // Прикладная дискретная математика. Приложение. 2018. № 11. С. 57–61.
4. *Jimenez R. A.* Generation of 8-bit s-boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit s-boxes and Finite Field Multiplication. Havana: Havana University, Institute of Cryptography, 2017. http://www.cs.haifa.ac.il/~orrd/LC17/paper60.pdf
5. *Fomin D. B.* New Classes of 8-bit Permutations Based on a Butterfly Structure. CTCrypt. Suzdal, 2018. https://ctcrypt.ru/files/files/2018/09_Fomin.pdf

6. *Wood C. A.* Large Substitution Boxes with Efficient Combinational Implementations. Thesis. Rochester Institute of Technology, 2013.
7. *Daemen J. and Rijmen V.* The Design of Rijndael, AES — the Advanced Encryption Standard. Springer Verlag, 2002.
8. *AlTawy R. and Youssef A. M.* A meet in the middle attack on reduced round Kuznyechik // IEICE Trans. 2015. V. 98-A. P. 2194–2198.
9. *Park S., Sung S.H., Lee S., and Lim J.* Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES // LNCS. 2003. V. 2887. P. 247–260.

УДК 519.17 DOI 10.17223/2226308X/12/33

ОЦЕНКА ХАРАКТЕРИСТИК ПЕРЕМЕШИВАНИЯ ХЭШ-ФУНКЦИЙ СЕМЕЙСТВА MD

А. М. Коренева

Матрично-графовый подход (МГП), нашедший успешное применение к оценке свойств итеративных блочных шифров и генераторов ключевого расписания, впервые представлен как инструмент оценивания перемешивающих свойств алгоритмов хэширования. Особенность применения МГП к хэш-функциям связана с неочевидностью построения перемешивающих матриц, характеризующих зависимость битов сгенерированного хэш-значения от битов исходного сообщения. Для хэш-функций MD4, MD5, SHA-1, SHA-256 построены перемешивающие матрицы порядка $512 + n$, где n — длина блока, с которым оперирует односторонняя функция сжатия алгоритма хэширования при обработке 512-битового блока входного сообщения ($n = 128$ для MD4 и MD5, $n = 160$ для SHA-1 и $n = 256$ для SHA-256). К исследованным характеристикам перемешивания относятся локальные экспоненты перемешивающих матриц, то есть для каждой матрицы M определено наименьшее натуральное число γ, такое, что при любом натуральном $\tau \geqslant \gamma$ положительны все столбцы матрицы M^τ с номерами $513, 514, \ldots, 512 + n$. Значения локальных экспонентов являются нижними оценками числа итераций, после которых каждый бит сгенерированного хэш-значения может существенно зависеть от всех битов исходного сообщения. Полученные значения ($\gamma = 21$ для MD4, MD5, SHA-256 и $\gamma = 23$ для SHA-1) косвенно свидетельствуют о схожих криптографических качествах рассмотренных алгоритмов хэширования, несмотря на варианты их усиления за счёт увеличения длины блока и усложнения функции сжатия.

Ключевые слова: *алгоритмы хэширования, структура Меркла — Дамгарда, матрично-графовый подход, перемешивающие свойства.*

Введение

В основе принципа перемешивания, важного для многих криптографических алгоритмов, лежит существенная нелинейная зависимость выходных данных от элементов входа. Для оценки множества существенных переменных композиции преобразований векторного пространства применяется матрично-графовый подход, теоретические основы которого изложены в [1]. Глубина итерации преобразования, при которой каждый бит выходного значения может зависеть от всех битов входа, оценивается снизу значением экспонента примитивного перемешивающего орграфа. В течение последних лет МГП нашёл успешное применение для исследования свойств итеративных блочных шифров и генераторов ключевого расписания [2 – 4], для которых перемешиваю-